INSIDER THREAT INCIDENTS REPORT
FOR
July 2024

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

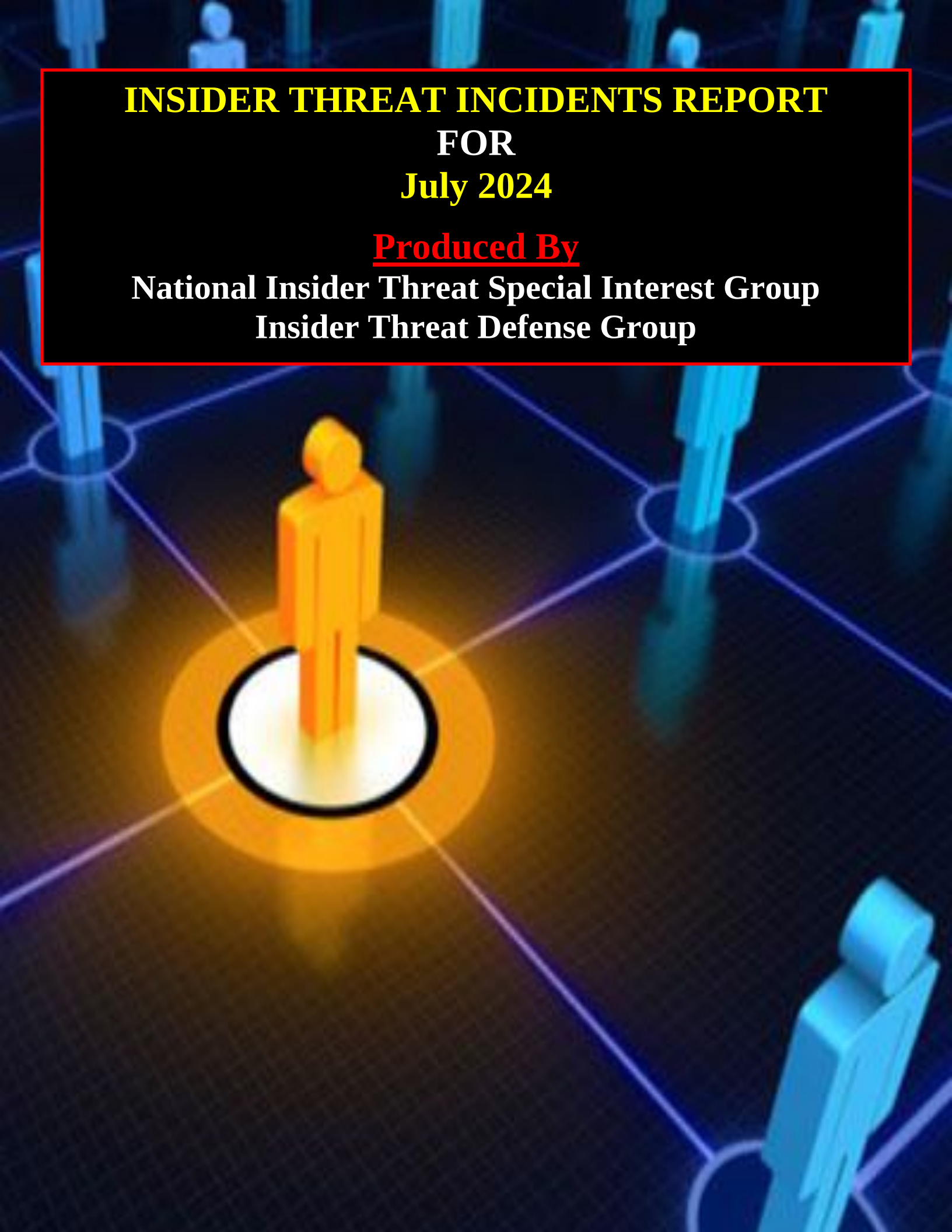

TABLE OF CONTENTS

PAGE

Insider Threat Incidents Report Overview ……. 3

Insider Threat Incidents For March 2024 …….. 4

Definitions of Insider Threats …… 27

Types Of Organizations Impacted …… 27

Insider Threat Damages / Impacts Overview ……... 28

Insider Threat Motivations Overview ……... 29

What Do Employees Do With The Money They Steal / Embezzle From Companies / Organizations …… 30

2024 Association Of Certified Fraud Examiners Report On Fraud …….. 31

Fraud Resources …….. 32

Severe Impacts From Insider Threat Incidents …… 33

Insider Threat Incidents Involving Chinese Talent Plans …… 54

Sources For Insider Threat Incidents Postings ……. 56

National Insider Threat Special Interest Group Overview ……..57

Insider Threat Defense Group - Insider Risk Management Program Training & Consulting Services Overview …… 59

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 **5,500+** 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, embezzlement, contracting fraud, bribery and kickbacks. This very evident in the Insider Threat Incidents Reports that are produced monthly by the NITSIG and the ITDG.

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

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

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

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

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

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

These monthly reports are recognized and used by Insider Risk Program Managers and security professionals working for major corporations, as an educational tool to gain support from CEO's, C-Suite, key stakeholders and supervisors for Insider Risk Management (IRM) Program's. The incidents listed on pages **4 to 24** of this report provide the justification, return on investment and the funding that is needed for an IRM Program. These reports also serve as an excellent Insider Threat Awareness Tool, to educate employees' on the importance of reporting employees' who may pose a risk or threat to the organization.

INSIDER THREAT INCIDENTS
FOR JULY 2024

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

Australian Soldier & Husband Arrested & Charged With Spying For Russia - July 12, 2024

An Australian soldier and her husband have been arrested and each charged with spying for Russia.

Investigators say the couple both Russian born and Australian citizens obtained Australian Defence Force (ADF) material to share with Moscow. However, Australian police say "no significant compromise" of military secrets has been identified.

Kira Korolev, a 40-year-old army private, and her 62-year-old husband Igor Korolev were in court, each on one count of espionage.

Australian Federal Police (AFP) Commissioner Reece Kershaw said the couple had been in Australia for more than a decade before the alleged spying. Become citizens several years ago.

Igor worked as a self-employed laborer, and Kira was an information systems technician in the army, a role for which she had obtained a security clearance, police say.

Kira secretly traveled to Russia while on leave from the ADF, then instructed Igor to access her work account and send sensitive material so that she could forward it on to Russian authorities. (Source)

U.S. GOVERNMENT

2 U.S. Postal Workers Charged With Stealing U.S. Treasury Checks Valued At $4 Million+ - July 10, 2024

Between June 2021 and August 2023, Kevaughn Wellington and Ky-Mani Straker (USPS Employees) engaged in a scheme to steal and sell Treasury checks intended for, among other things, individuals entitled to Social Security benefits, COVID-19 stimulus checks and tax refunds. Wellington stole parcels containing Treasury checks from the JFK Mail Facility where he was employed at the time as a postal worker. Then, together with Straker and others, Wellington sold the stolen Treasury checks for a cut of the profit.

As part of the scheme, Wellington and Straker stole over 125 Treasury checks valued at more than $4 million. Straker falsely endorsed and deposited stolen Treasury checks in a bank account and withdrew the deposited funds for his own financial gain. (Source)

Former U.S. Postal Service Maintenance Manager Sentenced To Prison For Stealing $6,500 In Cash - July 26, 2024

Barry Gallon was employed as a Maintenance Manager at the United States Postal Service's Indianapolis Processing and Distribution Center for seven years.

Between August 31, 2023, and September 20, 2023, Gallon stole cash from letters, packages, bags, and mail while working at the distribution center. The total amount of money stolen by the defendant was found to be no more than $6,500. (Source)

Department Of Agriculture Employee Pleads Guilty To Role In $1 Million Fraud & $500,000 Bribery Scheme To Benefit His Private Company - July 8, 2024

Between 2018 and 2023 Ifediora Oli was employed at the United States Department of Agriculture (USDA). He was separately acting as the Principal of Highbury Global Group, Inc. (Highbury).

Bridgette Crowell and Obinna Ogbu pleaded guilty to conspiring with Oli to defraud the District Of Columboa and the Washington Metropolitan Area Transit Authority (WMATA).

Ogbu was employed at WMATA as an information technology (IT) customer support manager who sometimes also served as a WMATA contracting officer's technical representative (COTR) on certain WMATA contracts. Crowell was a public employee who managed contracts at the District's Office of Contracting and Procurement (OCP) and, before that, WMATA.

Beginning in 2018, Oli and Ogbu agreed to use Ogbu's official position and connection to Crowell to steer funds from WMATA IT-related contracts to Highbury. As part of the conspiracy, Oli and Ogbu agreed to commit bribery. Specifically, Oli and Ogbu agreed that Oli would give Ogbu things of value in exchange for Ogbu misusing his position at WMATA to benefit Oli. By 2023, Oli and Highbury had received nearly $500,000 through this corrupt scheme. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Former CIA / White House Employee Arrested For Acting As An Agent Of South Korean Government In Return For Personal Enrichment - July 17, 2024

Sue Mi Terry, a former CIA and White House employee, subverted foreign agent registration laws in order to provide South Korean intelligence officers with access, information, and advocacy. Terry allegedly sold out her positions and influence to the South Korean government in return for luxury handbags, expensive meals, and thousands of dollars of funding for her public policy program.

After leaving U.S. government service and for more than a decade, Terry worked as an agent of the government of the Republic of Korea (ROK), commonly known as South Korea, without registering as a foreign agent with the Attorney General, as required by law. As covertly directed by ROK government officials, Terry publicly advocated ROK policy positions, disclosed non-public U.S. government information to ROK intelligence officers, and enabled ROK officials to gain access to U.S. government officials. In return for these actions, ROK intelligence officers provided Terry with luxury goods, expensive dinners, and more than $37,000 in funding for a public policy program focusing on Korean affairs that Terry controlled.

From in or about 2001 to in or about 2011, Terry served in a series of positions in the U.S. government, including as an analyst on East Asian issues for the Central Intelligence Agency, as the Director for Korea, Japan, and Oceanic Affairs for the White House National Security Council, and as the Deputy National Intelligence Officer for East Asia at the National Intelligence Council. Since leaving government service in or about 2011, Terry has worked at academic institutions and think tanks in New York City and Washington, D.C. Terry has made media appearances, published articles, and hosted conferences as a policy expert specializing in, among other things, South Korea, North Korea, and various regional issues impacting Asia. Terry has also testified before Congress on at least three occasions regarding the U.S. government's policy toward Korea. (Source)

U.S. Army Civilian Employee Sentenced To Prison For $100 Million Fraud Scheme / Used Funds For Jewelry, Clothing, Vehicles, Real Estate - July 23, 2024

Janet Mello worked as a Financial Program Manager for the U.S. Army, Installation Management Command – G9 (Morale, Welfare and Recreation) Child and Youth Services (CYS) at Fort Sam Houston, in Texas

In or around December 2016 through at least August 29, 2023, Mello formed a business she called Child Health and Youth Lifelong Development (CHYLD). The sole purpose of CHYLD was to receive grant funds from the 4-H Military Partnership Grant program, which Mello fraudulently secured by way of her position as a CYS financial program manager.

Once Mello received a grant check, she deposited the check into her bank account, spending the money on clothing, jewelry, vehicles and real estate. Mello repeated the process 49 times during a six-year period, requesting approximately $117,000,000 in payments, and receiving approximately $108,917,749. (Source)

Defense Of Department Employee Pleads Guilty To $624,000+ Fake Invoices Scheme - July 1, 2024

Zelene Charles, a previous civilian employee of the Department of Defense, at the Defense Language Institute in Monterey, California, perpetrated a scheme to defraud the U.S. government by creating fake purchase requests and invoices for government purchases from both fictitious and legitimate business entities.

The items listed in these invoices were never actually purchased or received by the government. Between December 2016 and April 2020, Charles placed approximately 185 fraudulent charges, causing a total loss to the government of $624,250.

To conceal that she was the recipient of the stolen funds, Charles frequently renamed the business names associated with intermediary accounts and, in total, used at least 78 different account names. (Source)

Shipyard Contractor Sentenced To Prison For Stealing Almost $600,000 Worth Of Computer Equipment From U.S. Navy - July 10, 2024

Ernesto Saldivar was a civilian contractor at General Dynamics who was employed as part of the shipyard's modernization efforts. ,

From November 2022 to August 2023, Saldivar stole hundreds of military hard drives and laptops from declassified areas on ships undergoing maintenance. Saldivar then sold the stolen items on eBay. Two of the hard drives he stole contained classified military communications. The affected ships included the USS Pinckney, USS Curtis Wilbur and USS Spruance. The total value of the stolen computer equipment – including two laptops, two programmer units, four DC-DC converters, 18 power converters, and 302 hard drives – totaled $596,997.53.

During the investigation of the missing hard drives, the U.S. Army Criminal Investigation Laboratory conducted a forensic analysis on fingerprints left inside the empty hard drive trays. These interior areas of the hard drive trays could only be touched after a hard drive was removed. The prints belonged to Saldivar. Naval Criminal Investigative Service agents also traced eBay listings of some of the stolen equipment to Saldivar. And, during a court-authorized search of Saldivar's home on August 25, 2023, NCIS agents recovered 120 of the missing hard drives, a Panasonic Toughbook laptop from the USS Pinckney with software from Integrated Voice Communications System (IVCS), several DC-DC converters traceable to the USS Pinckney, a BPM Microsystems 1410 taken from the Curtis Wilbur, and a BPM Microsystems 1710 Universal Device Programmer matching the serial number of an inventoried loss, all stored haphazardly in a shed on Saldivar's property. (Source)

Employee Of Armed Forces Recreation Center Pleads Guilty Theft Of $183,000+ - July 9, 2024

Elizabeth Carpenter was employed as an accounting technician by Shades of Green, an Armed Forces Recreation Center resort owned by the Department of Defense (DOD) located on Walt Disney World Resort property in Lake Buena Vista.

Between July 13, 2022, and March 19, 2024, Carpenter used her position as a DOD employee with computer credentials to access guest accounts to refund a portion of guests' room payments to Carpenter's personal credit card accounts. Carpenter engaged in at least 652 unauthorized transactions totaling approximately $183,079. (Source)

Former National Security Agency Contractor Sentenced To Prison For $176,000+ Time & Attendance Fraud - July 3, 2024

Jacky McComber was the Chief Executive Officer of an information technology company that had contracts with the NSA. Because the subject matter of these contracts involved classified information, most of the work had to be performed at a secure location, and there were significant limitations to the amount of work that could be performed off-site.

McComber billed for her supposed work physically at the NSA, when in reality approximately 90% of the work she billed for was not when she physically was at the NSA. The evidence further showed that McComber at times did not work the number of hours on the contract that she recorded on her timesheets.

For example, on occasions when McComber billed a full day to the contract, she participated in charity events, attended a reunion, and was on vacation. As further detailed in trial testimony, McComber participated in a voluntary interview with NSA-OIG investigators as a result of information received from a whistleblower indicating that McComber was billing the government for hours that she was not actually working.

McComber was odered to pay $176,913 in restitution for submitting false invoices to the National Security Agency (NSA) for overstating her hours worked on a contract and for making false statements to investigators from the NSA's Office of the Inspector General. (Source)

U.S. Army Research Biologist Pleads Guilty To Accepting $40,000 In Bribes In Exchange For Favorable Action On Contracts - July 1, 2024

Jason Edmonds was employed by the United States Army as a Research Biologist at the U.S. Army Combat Capabilities Development Command (CCDC) Chemical Biological Center (CB Center) located at the Aberdeen Proving Ground (APG) in Marylan. The CCDC CB Center was the nation's principal research and development center for non-medical chemical and biological weapons defense. The CB Center developed technology in the areas of detection, protection, and decontamination.

From 2012 to 2019, Edmonds accepted cash and other financial benefits from John Conigliaro, the owner and CEO of EISCO, Inc. in exchange for favorable action on CB Center contracts. For example, in July 2013, Edmonds directed a $300,000 CB Center project to EISCO. Three months later, in October 2013, Conigliaro gave Edmonds $40,000 in cash so that Edmonds could purchase two rental real estate properties. Once Edmonds purchased the rental properties, Conigliaro paid for thousands of dollars of renovations to the rental properties.

Relative to the cash exchange, Edmonds and Conigliaro executed a "Promissory Note," which was subsequently amended by Edmonds on June 14, 2014.

In the amended "Promissory Note," Edmonds credited himself $18,100 against the $40,000 in cash for past projects that Edmonds had directed to EISCO at the CB Center.

Edmonds also wrote that Conigliaro would provide him an additional $25,000 in exchange for future projects that Edmonds would direct to EISCO.

Between December 2016 and August 2017, Edmonds directed a series of government projects to EISCO in exchange for a stream of benefits from Conigliaro, including a kitchen remodel at Edmonds's personal residence, the purchase of a granite countertop, a kitchen sink, and new siding to his home. (Source)

Air Force Base Employee Charged With Obstructing A Criminal Investigation Into Cause Of 2017 Military Plane Crash Killing 16 Service Members - July 10, 2024

On July 10, 2017, a United States Marine Corps KC-130 transport aircraft known as Yanky 72 crashed near Itta Bena, Mississippi, resulting in the death of fifteen Marines and one Navy Corpsman.

James Fisher is a former propulsion engineer with the C-130 program office at Robins Air Force Base, engaged in a pattern of conduct intended to avoid scrutiny for his past engineering decisions related to why the crash may have occurred. Specifically, the indictment alleges that Fisher knowingly concealed key engineering documents from criminal investigators and made materially false statements to criminal investigators about his past engineering decisions. (Source)

U.S. Army Reserve Officer Admits To Military Pay Fraud Of $140,000+ - July 19, 2024

Captain Jean Philippe Martial worked as a U.S. Army Reservist from Utah's 76th Operational Response Command. He was indicted for military pay fraud that occurred at Fort Douglas, Utah, during the coronavirus pandemic.

Captain Martial defrauded the United States out of more than $140,000 in unearned military pay entitlements from June 2019 to September 2021. Last month, Colonel Reece Roberts, formerly of Utah's 76th Operational Response Command, pled guilty to filing a fraudulent claim against the United States, conspiring to defraud the United States, and other federal crimes. (Source)

Active Duty Army & Former Marine Reserve Indicted & Arrested For Drug Distribution - July 11, 2024

From August 2021 through June 2024, Davud Gonzalez knowingly and intentionally conspired with others to distribute heroin, fentanyl, and methamphetamine. He was additionally charged with maintaining residences in Tulsa for drug distribution. (Source)

Former Army Officer / JAG Attorney Pleads Guilty To Destruction Of U.S. Army Property & Lying To Investigators About Contacting Russian Embassy - July 24, 2024

In February 2022, Manfredo Madrigal was assigned to a staff position at the Judge Advocate General (JAG) School in the Training Developments Directorate, whose mission was to design and develop training products for the JAG Corps and the Army. Madrigal possessed an active security clearance and previously served overseas on sensitive operations.

In early 2022, Madrigal was under investigation by the U.S. Army and the JAG School for failing to report a previous conviction for driving under the influence (DUI).

While his Army investigation was pending, Madrigal deleted, without authorization, online JAG training materials and filmed himself doing so while graphically describing his ill-will towards the Army. The FBI's investigation also revealed that Madrigal made a phone call to the Russian embassy in Washington, DC the same night that he deleted the training materials and then texted a witness that Russia wanted to know what he knew.

On February 22, 2022, Madrigal was discharged from the JAG School and claimed in his exit paperwork that he had no unreported contact with a foreign national. In April and May 2022, Madrigal was interviewed by the FBI about his actions. In these interviews, Madrigal made multiple false statements regarding his actions, including denying any involvement in the deletion of materials and that he only learned of the deletion from a coworker, as well as falsely denying his contact with a foreign national at the Embassy. (Source)

Employees For Marine Equipment & Servicing Company Admit Roles In Scheme To Defraud Department Of Defense - July 23. 2024

From March 2016 through April 2020, Linda Mika (Mother) and Kenneth Mika (Son) conspired with each other and others to defraud the DoD and one of its combat logistic support arms, the Defense Logistics Agency (DLA), by engaging in a pattern of unlawful product substitution. The Mikas were employees of Monmouth Marine Monmouth Marine Engines Inc. (Monmouth Marine), a maritime equipment and servicing facility, which, as an approved federal contractor, also entered into contracts with DLA to supply DoD contracting entities with replacement hardware for DoD's military branches.

The Mikas, on behalf of Monmouth Marine, obtained contracts with the DoD by falsely claiming that the military parts they contracted to provide would be exact products furnished by authorized manufacturers or suppliers. Once awarded the contracts, however, the Mikas sourced non-conforming substitute parts at a significantly reduced cost to fill the contracts. They did this to maximize their profit margin while also suppressing fair competition in the bidding of federal contracts. Upon receipt by Monmouth Marine, the non-conforming parts were then shipped to DLA or various military purchasers in packaging disguising the parts' identities in an effort by the Mikas to deceive DLA and its unwitting downstream purchasers. (Source)

CRITICAL INFRASTRUCTURE

Federal Air Marshal Admits To The Unauthorized Selling Of DHS Family ID Cards - July 18, 2024

Jonathan Ledesma is a U.S. Air Marshal.

From October 2021 through January 2023, Ledesma purchased cards that identified their bearers as being a "family member" of "Jonathan J. Ledesma," a "Federal Officer." These cards were each embossed with the apparent insignia of DHS as well as a QR code that was linked to Ledesma's cellular phone. Though Ledesma was not authorized to sell the insignia of DHS, or any colorable imitation of the insignia, Ledesma then sold the cards to others.

In July 2022, Ledesma sold a card to a person who was arrested on Jan. 30, 2023, while in possession of the card. A federal officer scanned the QR code and spoke with Ledesma, who indicated that he had provided the card to person because he was a friend and business associate of the person's father. This statement was false because, as Ledesma well knew, he had never met or done business with person's father. On Jan. 18, 2023, Ledesma sold a second card to another individual. (Source)

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

TSA Employee Indicted After Bomb Hoax At Airport - July 9, 2024

Tulsa International Airport Police received a report of a bomb threat on a handwritten note that was located in the pre-security side of the airport. Airport police immediately responded and secured the area and determined that there was no threat to public safety. Airport police then conducted an investigation where they identified a possible suspect and contacted the Tulsa FBI office. Tulsa FBI took over the investigation from that point forward and proceeded with their own investigation.

A TSA employee Sharon Devine left a note in the restroom on March 5, 2024, and March 23, 2024. The notes stated there was a bomb located in the airport. (Source)

Police Sergeant Sentenced To Prison For $16,000+ Overtime Fraud Scheme / 12 Other Officers Charged - July 23,2024

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

Between March 2015 and December 2016, Finch personally collected approximately $16,151 for overtime hours he did not work.

To date, over a dozen Boston Police officers have been charged in connection with committing overtime fraud at the Boston Police Department's evidence warehouse. (Source)

Police Officer Sentenced For $16,000+ Overtime Fraud Scheme - July 13, 2024

From February 2015 through February 2018 Thomas Nee submitted false and fraudulent overtime slips for overtime shifts that he did not work at the evidence warehouse.

Nee personally collected approximately $16,151 for overtime hours he did not work. (Source)

Police Officer Sentenced To Prison For Conducting Illegal Traffic Stops To Steal Cocaine - July 2, 2024

Frenel Cenat is a former police officer with the City of Miami Police Department (MPD).

Cenat used his police position and authority, and his unmarked MPD-issued vehicle and equipment to conduct two illegal traffic stops to steal what he believed were drug proceeds and seven kilograms of cocaine from the drivers.

A confidential human source (CHS) stated to law enforcement that they had been told by a mutual friend that Cenat had previously conducted traffic stops of individuals known to have engaged in drug transactions for the purpose of stealing the drugs and/or money those individuals were transporting.

On Oct. 16, 2023, the friend introduced Cenat to the CHS at a meeting in Broward County, during which the three of them discussed an opportunity for Cenat to use his police officer position to stop an individual immediately following a drug transaction and steal approximately $50,000 in drug proceeds that the individual would have in their vehicle. Cenat indicated that he conducts the traffic stops outside of his jurisdiction and while off duty. (Source)

Baltimore Police Officer Sentenced To Prison For Drug & Firearms Distribution - July 1, 2024

Steven Angelini was a member of the Baltimore Police Department (BPD) and from January 2022 through May 2022.

Angelini and his Co-Conspirator 1 conspired to distribute cocaine and oxycodone. During the conspiracy Angelini twice also offered to go to the Baltimore City Police Department (BPD) Homicide Unit to obtain information about an investigation involving Co-Conspirator 1's supplier who had been murdered.

Angelini's offer to obtain the video for Co-Conspirator 1 was made with the sole objective to persuade Co-Conspirator 1 to provide him with cocaine.

In April 2022, Angelini provided 20 oxycodone pills to Co-Conspirator 1. Later in April 2022, Angelini texted Co-Conspirator 1 that he was at a gun shop and stated that he wanted to purchase cocaine from Co-Conspirator 1. Angelini then offered to purchase ammunition and firearms accessories for Co-Conspirator 1 in exchange for cocaine. Angelini purchased a magazine for the privately made firearm he sold to Co-Conspirator 1, as well as ammunition, including hollow-point ammunition, which he provided to Co-Conspirator 1 later that night in exchange for cocaine.

Angelini also provided Co-Conspirator 1 with law enforcement sensitive information on the case and some pictures, which were available to BPD employees through mass email dissemination. (Source)

Police Officer Charged In Insurance Fraud & Bribery Schemes Involving Homeowner - July 1, 2024

The indictment alleges that in 2019, Christian Claus, then a New Orleans Police Officer NOPD police officer, conspired with a New Orleans homeowner and a Nevada art appraiser to submit a fraudulent insurance claim on the homeowner's property.

The claim reported that valuable paintings were stolen from the insured's house, when in truth, the paintings were neither valuable nor stolen. The indictment also alleges that the homeowner agreed, in exchange for Claus using his police position to further the scheme, to share the insurance proceeds with Claus and to provide Claus with assistance in obtaining employment positions. (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

Former Office Of Emergency Medical Services Associate Director Pleads Guilty To Embezzling $4.3 Million+ From Virginia Department Of Health Using Shell Company - July 26, 2024

Used Funds For The Purchase Of Real Estate, Luxury Vehicles, Firearms, Jewelry

Beginning on August 10, 2013, Adam Harrell was an employee of the Virginia Department Of Health (VDH). On September 10, 2019, he became the Associate Director of the Office of Emergency Medical Services (OEMS). Harrell was responsible for managing Virginia's emergency response programs, epidemiology research, and the information technology systems that Virginia's emergency medical service providers rely on, among other responsibilities.

Harrell used his position to direct payments from VDH to a company he registered and controlled, Strategic Tech Innovations, LLC. Harrell concealed his ownership of and affiliation with Strategic Tech from VDH and OEMS, and used this entity to embezzle funds from his employer through two separate means.

From January 2021 through May 2023, Harrell created 15 fraudulent invoices for services and technology that Strategic Tech would purportedly provide to OEMS.

Harrell set exorbitant and non-market prices for the various line items on the invoices, knowing the vast majority of those items would not be provided by Strategic Tech. Without OEMS's knowledge or approval, Harrell would submit these fraudulent invoices to the Western Virginia EMS Council (WVEMS), a regional emergency medical services council that serves as a pass-through for OEMS payments to vendors. Each of these invoices were paid by WVEMS with OEMS funds. By directing the invoices to WVEMS instead of Accounts Payable at OEMS, Harrell circumvented the requirement that Strategic Tech be approved as a vendor to VDH and OEMS and evaded scrutiny by the Accounts Payable department. As the Associate Director of OEMS, Harrell was able to unilaterally approve the same fraudulent Strategic Tech invoices he drafted.

Harrell deposited each of the checks he illegally received from WVEMS into the Strategic Tech checking account he controlled and used the funds for personal expenses, including the purchase of real estate, luxury vehicles, dozens of firearms, and jewelry. In total, Harrell received $4,337,395 in OEMS funds. (Source)

Asset Manager Director For Housing Authority Sentenced To Prison For Role In $3 Million+ Contracting Fraud Scheme - July 25, 2024

From approximately 2015 through 2019, Albert Smith served as the Asset Manager Director for the Housing Authority of South Bend (HASB), in Indiana. Smith reported directly to the Executive Director of HASB.

Smith was found guilty of conspiring with those at the HASB and with outside contractors to defraud the HASB. The fraud scheme involved the issuance of HASB payment checks to four outside contractors for contracting work that had not actually occurred. These contractors would then deposit the HASB payment checks, withdraw a portion of each check in cash, and hand-deliver the cash back to co-conspirators at the HASB's main office. Smith was involved in creating hundreds of fraudulent documents to conceal the fraud. (Source)

State Representative Sentenced To Prison For Accepting Bribes From Casino / Promise Of Future Employment With $350,000 Salary - July 11, 2024

From 2006 to 2022, Sean Eberhart served as the elected representative of Indiana House District 57, which includes Shelby County and portions of Bartholomew and Hancock counties, in Indiana. During his tenure, Eberhart served as a member of the House Committee on Public Policy, which has jurisdiction over matters concerning casinos and gaming in Indiana.

From January to May of 2019, Eberhart conspired with Individual A to devise a scheme to use Eberhart's official elected position to benefit that person's company, Spectacle Entertainment. Spectacle Entertainment was formed by Individual A after Centaur, a company that owned and operated off-track betting facilities in Indiana, including the Shelbyville Casino in Eberhart's District, was acquired by Caesars Entertainment in July of 2018. After that acquisition, Individual A formed Spectacle Entertainment and many of the same executives of Centaur continued in substantially similar roles as executives of Spectacle.

As part of the illegal scheme, Eberhart agreed to use his position in the Indiana House of Representatives to advocate and vote for a Gaming Bill that positively impacted Spectacle.

Terms in the bill would authorize the transfer of the licenses for two casinos on Lake Michigan to Spectacle's ownership in Gary and Terre Haute, Indiana, while reducing the usual $100 million transfer fee that Spectacle was originally set to pay, to only $20,000.

On March 27, 2019, during an Indiana House Public Policy Committee hearing, Eberhart vocally advocated to remove the $1 million transfer fee from the Gaming Bill entirely.

At a hearing on April 23, 2019, hearing, Eberhart advocated in favor of a 20% tax rate that would save Spectacle tens of millions of dollars. The next day, Eberhart voted in favor of the Gaming Bill and those associated tax provisions.

In return for his advocacy and vote for the Gaming Bill, Eberhart accepted the promise of future employment at Spectacle, which included an annual salary of $350,000 and equity stake in the company. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

Former Graduate School Assistant Dean And 2 Other Employees Admit To Embezzling $1.3 Million+ For 12 Years For Personal Use - July 26, 2024

Between 2009 and July 2022, Teresina DeAlmeida, Rose Martins, and Silvia Cardoso conspired to fraudulently misappropriate more than $1.3 million from their former employer, a graduate school of a university in Essex County, New Jersey. DeAlmeida was an Assistant Dean responsible for financial functions, and Martins served as her assistant. Cardoso, DeAlmeida's sister, was also employed by the graduate school in a support staff role.

Beginning in 2009, DeAlmeida directed a graduate school vendor to pay Martins and Cardoso as though they worked for the vendor, even though they did not perform any services

From 2010 through 2022, DeAlmeida and Martins directed graduate school vendors to order hundreds of thousands of dollars of gift cards and prepaid debit cards the conspirators used for their personal benefit, and then to submit fraudulent invoices to the school purporting to be for goods and services that were never provided.

In 2015, Martins opened a shell entity called CMS Content Management Specialist LLC. Although CMS never rendered any services to the graduate school, Martins submitted, and DeAlmeida approved, fraudulent invoices totaling more than $208,000.

The conspirators also used DeAlmeida's school-issued credit card to make tens of thousands of dollars in unauthorized personal purchases. DeAlmeida and Martins used the card to make over $70,000 in purchases at an online retailer shipped directly to their homes, including woman's shoes, smart watches, and bed linens. DeAlmeida and Martins fraudulently altered certain receipts before submitting them to the school for payment. (Source)

University Employee Charged With Stealing $300,000 / Used Funds For TikTok Coins & Personal Expenses - July 23,2024

Kristen Battocletti is a former administrative assistant at St. Francis of Assisi University Parish in Tuscaloosa, Alabama.

Battocletti engaged in a scheme to defraud St. Francis of Assisi University Parish from April to October 2023. Battocletti stole approximately $300,000 from St. Francis, using the funds to purchase more than $220,000 in TikTok Coins and to pay personal expenses. Battocletti used the TikTok Coins to send digital gifts to TikTok content creators. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

Bank Manager Sentenced To Federal Prison For Stealing $345,000+ - July 10, 2024

Between June 2023 and September 2023, Jessica Marshall was working as a Bank Manager at the Bank of Idaho's downtown Spokane, Washington branch.

Using her position as a manager, Marshall stole and embezzled at least $345,664 in cash from the bank vault, ATM, and her cash drawer.

Marshall falsified documents to reconcile the cash and directed bank employees to sign falsified count sheets in order to hide her theft and embezzlement. Marshall also used her position as Bank Manger to make fraudulent deposit transactions into her spouse's account. These fraudulent transactions reflected that money was being deposited into the account; however, no funds were deposited.

When Bank of Idaho inquired about the deposits into her spouse's account, Marshall attempted to conceal her conduct by using a co-worker's email account to send an e-mail with false information. Marshall then accessed the computer of another co-worker to delete an email from Bank of Idaho inquiring about the deposits. (Source)

Regions Bank Branch Manager Charged With Embezzling $250,000 / Used Funds To Make Payments On House & Car - July 9, 2024

Eric Schouest admitted to stealing $250,000 from customers during his time as a Branch Manager at the Regions Bank in Louisiana.

Schouest used his power to embezzle by indulging in a data breach accessing customers' details. He illegally accessed customers' accounts, both open and closed accounts. He then transferred funds in and out of customers' accounts and stole $250,000 worth of money.

The illegal exploitation started in 2020 and was in operation until April 2021. He also sent false and fraudulent emails and forged documents to other Regions Bank employees to conceal his scheme. Some of the traceable fraudulent funds were used to make loan payments on personal items such as a house and a car. (Source)

Former Banker Extradited From United Kingdom To U.S. For Money Laundering & Bribing Ghanaian Officials For $70,000+ - July 16, 2024

Between December 2014 and March 2017, Asante Berko, an executive director in the Investment Banking Division of a wholly owned subsidiary of a U.S. global investment banking, securities, and investment management firm, allegedly conspired with others in connection with a multi-year bribery and money laundering scheme. During this time, Berko was a member of the team at the firm that was responsible for securing and managing a deal between its client, a Turkish energy company, and the Republic of Ghana to build a power plant in Ghana and to provide financing for the plant. Berko and others allegedly offered and paid more than $70,000 in bribes to government officials in Ghana in exchange for their assistance in ensuring that the Turkish energy company was successful in winning the bid to build and operate the power plant. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Vice President Of Company Pleads Guilty To Role In Scheme To Illegally Export U.S. Avionics Equipment To Russia - July 2, 2024

Douglas Robertson is the former vice president of KanRus Trading Company Inc.

He pleaded guilty for his role in a years-long conspiracy to circumvent U.S. export laws by filing false export forms with the U.S. government and, after Russia's unprovoked invasion of Ukraine in February 2022.

Robertson continued to sell and export sophisticated and controlled avionics equipment to customers in Russia without the required licenses from the U.S. Department of Commerce.

In December 2023, Buyanovsky, the former President and owner of KanRus, pleaded guilty to conspiracy and money laundering and consented to the forfeiture of over $450,000 worth of avionics equipment and accessories, and a $50,000 personal forfeiture judgment.

On March 19, Chistyakov, a former KanRus broker, was arrested in Riga, Latvia, for his role in the illegal smuggling scheme. Chistyakov remains detained in Latvia pending extradition proceedings. (Source)

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

Telecommunications & Information Technology Worker Charged With Acting As Agent Of PRC Government - July 24, 2024

The indictment alleges that Ping Li was a U.S. citizen who immigrated to the United States from the PRC. At various times, Li worked for a major U.S. telecommunications company and an international information technology company.

From as early as 2012, Li allegedly served as a cooperative contact working at the direction of officers from the PRC's Ministry of State Security (MSS), to obtain information of interest to the PRC government. Li obtained a wide variety information at the request of the MSS, including information concerning Chinese dissidents and pro-democracy advocates, members of the Falun Gong religious movement, and U.S.-based non-governmental organizations, and to report that information to the MSS. Li also provided the MSS with information obtained from his employer. Li used a variety of anonymous online accounts for the purpose of communicating with the MSS, and traveled to the PRC to meet with the MSS. (Source)

North Korean Hackers Targeted Cyber Security Awareness Training Firm KnowBe4 Into Hiring Fake IT Worker From North Korea – July 2024

Cybersecurity awareness training company KnowBe4 has revealed it was duped into hiring a fake IT worker from North Korea, resulting in attempted insider threat activity.

The malicious activity was identified and prevented before any illegal access was gained or any data was compromised on KnowBe4 systems.

In a blog published on July 23, 2024, KnowBe4 detailed the high level of sophistication used by North Korean attackers in creating a believable cover identity, capable of passing an extensive interview and background check.

The case demonstrates North Korea's ongoing efforts to get fake workers employed in IT roles in Western companies, both as a means of generating revenue for the Democratic People's Republic of Korea (DPRK) government and to conduct malicious cyber intrusions.

Stu Sjouwerman, Chief Executive Officer and President at KnowBe4, noted: "This is a well-organized, state-sponsored, large criminal ring with extensive resources. The case highlights the critical need for more robust vetting processes, continuous security monitoring, and improved coordination between HR, IT and security teams in protecting against advanced persistent threats."

The article goes into detail about how the fake IT worker gained employment and when KnowBe4 started detecting suspicious activity. (Source)

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

Vice President Of Drug Company Indicted In Scheme To Distribute Drugs Using False Prescriptions / Company Fined $16.9 Million - July 9, 2024

Beginning in approximately 2015, while U.S. Compounding, Inc. (USC) was still a privately-held corporation, a USC sales representative (Sales Rep 1) entered into an illegal arrangement with a veterinarian, wherein Sales Rep 1 would use the Veterinarian's state veterinary licenses to generate false prescriptions in order to justify shipping prescription drugs directly to consumers, including to consumers in the Southern District of New York, in violation of the FDCA.

Those consumers otherwise lacked bona fide prescriptions for those drugs.

The Veterinarian was promised a 10% commission of all such sales generated using his credentials, even though Sales Rep 1 and his supervisor, Sam Glover the Vice President of Sales at USC, knew that the prescriptions issued in the Veterinarian's name

were a sham. Glover, Sales Rep 1, and the sales team working under them generated approximately $1 million in sales annually because of the false prescription scheme, which comprised approximately one-third of Sales Rep 1's total sales of USC drugs.

Pursuant to the plea agreement, USC agreed that it is subject to an approximately $4.2 million forfeiture payment and a criminal fine of up to $16.9 million. (Source)

Hospital Chief Financial Officer & 3 Others Charged In $15+ Million Embezzlement Scheme - July 12, 2024

Anosh Ahmed was the Chief Financial Officer of a Chicago hospital. He was responsible for managing the hospital's finances, including its Finance, Accounting, and Accounts Payable departments.

From 2018 to 2022, Ahmed schemed with the hospital's Chief Transformation Officer, Heather Bergdahl, and the medical supply company owner, Sameer Suhail to cause the hospital to issue payments to vendor companies for purported goods and services that they knew had not been provided.

Many of the vendor companies were created by Suhail and Ahmed under various names to conceal their association with the fraudulent payments. Bergdahl opened bank accounts in the names of two legitimate hospital vendors and caused the hospital to deposit fraudulent payments into those accounts, the indictment states.

Ahmed, Bergdahl, and Suhail allegedly created fictitious invoices, payment requests, delivery receipts, and other false documents about goods and services purportedly provided to the hospital. As a result of the scheme, the defendants caused the hospital to pay more than $15 million into bank accounts that they controlled. (Source)

Doctor Who Worked For 2 Hospice Organizations Pleads Guilty To $3.2 Million+ Medicare Health Care Fraud Scheme - July 24, 2024

A Ventura County physician who worked for two Pasadena hospices pleaded guilty to defrauding Medicare out of more than $3 million by billing the public health insurance program for medically unnecessary hospice services.

From July 2016 to February 2019, Contreras and co-defendant Juanita Antenor, schemed to defraud Medicare by submitting nearly $4 million in false and fraudulent claims for hospice services submitted by two hospice companies: Arcadia Hospice Provider Inc., and Saint Mariam Hospice Inc. Antenor controlled both companies.

Medicare only covers hospice services for patients who are terminally ill, meaning that they have a life expectancy of six months or less if their illness ran its normal course.

Contreras falsely stated on claims forms that patients had terminal illnesses to make them eligible for hospice services covered by Medicare, typically adopting diagnoses provided to him by hospice employees whether or not they were true. Contreras did so even though he was not the patients' primary care physician and had not spoken to those primary care physicians about the patients' conditions. Medicare paid on the claims supported by Contreras' false evaluations and certifications and recertifications of patients.

In total, approximately $3,917,946 in fraudulently claims were submitted to Medicare, of which a total of approximately $3,289,889 was paid. (Source)

Office Manager For Medical Equipment Provider Indicted For $1.8 Million Health Care Fraud Scheme - July 18, 2024

Judy Strzelecki served as the Office Manager for A Woman's Place LLC, a durable medical equipment provider and retail shop in Downers Grove, Ill. A Woman's Place provided breast prostheses, compression garments, wigs, mastectomy bras, and other items to cancer survivors and women with chronic health conditions.

From 2015 to 2020, Strzelecki and others submitted fraudulent claims to Blue Cross and Blue Shield of Illinois and other health care benefit programs for equipment that was either not provided or was not medically necessary. Strzelecki and others also fraudulently billed the programs for more expensive products than were provided in order to seek higher reimbursement rates, the indictment states.

As a result of the scheme, Strzelecki and others fraudulently obtained at least $1.8 million in payments from health care programs for equipment that was not provided as billed, the indictment states. (Source)

Georgia Insurance Commissioner Sentenced To Prison For $750,000+ Healthcare Fraud & Kickback Scheme - July 12, 2024

John Oxendine abused his position as the former Georgia Insurance Commissioner by undermining the integrity of the state's healthcare system when he conspired with a physician to order hundreds of unnecessary and costly lab tests.

Oxendine conspired with Dr. Jeffrey Gallups and others to submit fraudulent insurance claims for medically unnecessary Pharmacogenetic, Molecular Genetic, and Toxicology testing.

Physicians associated with Dr. Gallups' ENT practice were pressured to order these medically unnecessary tests from Next Health, a lab in Texas. As part of Oxendine's healthcare fraud scheme, Next Health agreed to pay Oxendine and Dr. Gallups a kickback of 50 % of the net profit for eligible specimens submitted by Dr. Gallups' practice to the lab company.

The insurance companies paid more than $750,000 to Next Health because of these fraudulent claims. Next Health then paid $260,000 in kickbacks to Oxendine and Dr. Gallups.

To conceal the kickback payments, Oxendine and Dr. Gallups arranged for the payments to be made from Next Health to Oxendine Insurance Services, Oxendine's insurance consulting business.

Oxendine used a portion of the kickback money to pay a $150,000 charitable contribution and $70,000 in attorney's fees for Dr. Gallups. (Source)

Hospital Doctor Accessed 800 New Born Babies Medical Records So He Could Offer His Services At Private Clinic - July 26, 2024

800 people have received noticed from area hospitals that her baby's data was "inappropriately accessed" by a pediatrician within Windsor Regional Hospital (WRH)

In a statement sent to a TV News station, WRH confirmed a physician, who they have declined to identify, used the regional electronic medical records system without authorization in an effort to offer services at a private clinic. The individual began calling the parents of new borns to offer the clinics services, but blocked his number.

According to WRH, the physician in question has had their hospital privileges revoked. The matter has been reported to both the Information and Privacy Commissioner of Ontario and the College of Physicians and Surgeons of Ontario.

WRH said it's not clear how many newborns the pediatrician cold-called, but that letters were sent to those who gave birth to boys between January and May of this year – whether at Windsor Regional, Erie Shores HealthCare, or Chatham-Kent Health Alliance.

WRH says there is no evidence the physician "exported, printed, or otherwise electronically took personal health information from the hospital system, or retained any personal health information." (Source)

Hospital Doctor Convicted For Stealing Controlled Substances 6 Different Times - July 22, 2024
Dr. Nedza worked as a contract anesthesiologist at an Oklahoma City based hospital through March 2022.

Testimony presented at trial indicated that Dr. Nedza had exploited his role at the hospital to divert controlled substances, including fentanyl, ketamine, dilaudid, and midazolam, over a long period of time. Evidence presented at trial proved that, on at least six different occasions in early March 2022, Dr. Nedza pulled out large amounts of controlled substances by claiming the drugs were for patient surgeries. However, Dr. Nedza was not scheduled to perform, and did not perform those surgeries. Instead, he claimed to dispose of the drugs, but kept them for his own personal purposes. (Source)

Brightside Health On-Line Psychiatry Therapy Company Employee Allowed Wife To Impersonate Her For 2 Years - July 2, 2024
Brightside Health is a San Francisco company that offers nationwide online psychiatry and therapy sessions,

Hundreds of Americans may have unknowingly received therapy from an untrained impostor who masqueraded as an online therapist, possibly for as long as two years, and the deception crumbled only when she died, according to state health department records.

Peggy A. Randolph, a social worker who was licensed in Florida and Tennessee and formerly worked for Brightside Health, a nationwide online therapy company, is accused of helping her wife impersonate her in online sessions, according to an investigation report from the Florida Department of Health.

The report says the couple "defrauded" patients through a "coordinated effort": As Randolph treated patients in person, her wife pretended to be her in telehealth sessions with Brightside patients.

The deceit was discovered after the wife died last year and a patient realized they'd been talking to the wrong person, according to a Tennessee Department of Health settlement agreement.

Records from both states identify Randolph's wife only by her initials, T.R., but her full name is in her obituary: Tammy G. Heath-Randolph. Therapists are generally expected to have at least a master's degree, but Randolph's wife was "not licensed or trained to provide any sort of counseling services," according to the Tennessee agreement.

Randolph denies knowing that T.R. was using her Brightside Health Therapist Portal log-in credentials or treating clients under her account. However, she received compensation for the sessions conducted, the agreement states. (Source)

EMBEZZLEMENT / FINANCIAL THEFT / FRAUD / BRIBERY / KICKBACKS / EXTORTION / MONEY LAUNDERING / INSIDER TRADING / STOCK TRADING & SECURITIES FRAUD
Customer Service Employee For Business Telephone System Provider & 2 Others Sentenced To Prison For $88 Million+ Fraud Scheme To Sell Pirated Software Licenses - July 26, 2024
3 individuals have been sentenced for participating in an international scheme involving the sale of tens of thousands of pirated business telephone system software licenses with a retail value of over $88 million.

Brad and Dusti Pearce conspired with Jason Hines to commit wire fraud in a scheme that involved generating and then selling unauthorized Avaya Direct International (ADI) software licenses.

The ADI software licenses were used to unlock features and functionalities of a popular telephone system product called "IP Office" used by thousands of companies around the world. The ADI software licensing system has since been decommissioned.

Brad Pearce, a long-time customer service employee at Avaya, used his system administrator privileges to generate tens of thousands of ADI software license keys that he sold to Hines and other customers, who in turn sold them to resellers and end users around the world. The retail value of each Avaya software license ranged from under $100 to thousands of dollars.

Brad Pearce also employed his system administrator privileges to hijack the accounts of former Avaya employees to generate additional ADI software license keys. Pearce concealed the fraud scheme for many years by using these privileges to alter information about the accounts, which helped hide his creation of unauthorized license keys. Dusti Pearce handled accounting for the illegal business.

Hines operated Direct Business Services International (DBSI), a New Jersey-based business communications systems provider and a de-authorized Avaya reseller. He bought ADI software license keys from Brad and Dusti Pearce and then sold them to resellers and end users around the world for significantly below the wholesale price. Hines was by far the Pearces' largest customer and significantly influenced how the scheme operated. Hines was one of the biggest users of the ADI license system in the world.

To hide the nature and source of the money, the Pearces funneled their illegal gains through a PayPal account created under a false name to multiple bank accounts, and then transferred the money to investment and bank accounts. They also purchased large quantities of gold bullion and other valuable items. (Source)

Employee Sentenced To Prison For Role In Embezzling $4 Million+ In Elaborate Fraud, Extortion & Money Laundering Scheme - July 18, 2024

Gina Russell was sentenced to 125 months in prison for masterminding an elaborate fraud, extortion, and money laundering scheme, which resulted in a Maryland man embezzling more than $4 million from his Washington, D.C., employer. Russell is the sixth defendant to be sentenced in the case.

Russell met a New York woman in October 2009 in Manhattan and performed a psychic reading on her. Though Russell had no psychic powers, she convinced the New York woman that she did and told the woman that bad things would happen unless the woman raised large sums of money for Russell and her family. The woman started giving Russell money from her lawful jobs, but then Russell convinced her to lie to her father by claiming she needed money for therapy, extensive sleep studies, and university classes. After giving his daughter enormous sums of money, the New York woman's father eventually stopped providing her with financial assistance.

Russell then convinced the woman to earn more money through sex work. The woman advertised sensual massage services online, including Backpage.com. Through one of her ads, she met a Maryland man, who eventually fell in love with and proposed to her, even though he was married and had children. Preying on his affection, Russell and the New York woman conspired with Robert Evans, Tony John Evans, Corry Blue Evans, and Archie Kaslov to extort money and gold bars from the victim.

The New York woman told the Maryland man that she owed money to bad people from prior debts and that her life was in danger. As a result, the Maryland man embezzled more than $4 million from his employer between January and March of 2017. As part of the scheme, Russell had Tony John Evans impersonate a mobster during calls with the Maryland man.

During one of those calls, Tony John Evans asked if he needed to remind the Maryland man where his children went to school. Russell also dictated threatening texts and provided the New York woman with instructions on what to tell the Maryland man.

The Maryland man converted embezzled funds to cash and gold bars which he delivered to New York drop-off locations, including a hotel room, believing the funds were going to mobsters. In reality, all of the funds the man embezzled and delivered to New York went to members of the Russell-Evans-Kaslov family. (Source)

Employee Of Stock Broker-Dealer Firm Indicted For Role In $3.4 Million Insider Trading Scheme - July 18, 2024

Christopher Matthaei was a partner and senior salesperson at a Charlotte, North Carolina-based broker-dealer with offices in Red Bank, New Jersey.

From May 2020 through February 2021, Matthaei illegally traded on material, non-public information (MNPI) that he received from Sean Wygovsky, a conspirator and friend who worked at a large Canadian asset management firm. The MNPI pertained to Special Purpose Acquisition Companies (SPACs) that were engaged in confidential merger negotiations and shared information with the asset management firm as a potential investor in the SPAC deals.

Wygovsky received this MNPI every time a SPAC was placed on his firm's confidential restricted list, meaning that the firm's employees were prohibited from buying or selling the SPACs' securities, either personally or via another person or third party. Despite knowing about these trading restrictions, Wygovsky shared the MNPI with Matthaei, who then purchased securities in the SPACs using his personal brokerage accounts. In June 2020, Matthaei paid for a private plane and extended trip with Wygovsky and their families to a luxury resort on the island of St. Barts, where they continued to engage in the insider trading scheme.

In total, Matthaei made approximately $3.4 million in illegal trading profits from the insider trading scheme. (Source)

Fiscal Manager For Children's Advocacy Center Charged With $411,000+ Of Wire Fraud - July 26, 2024

From November 2018 to June 2022, while employed as the Fiscal Manager for the Children's Advocacy Center of Northeastern Pennsylvania (CAC / NEPA), Angela Saar engaged in a scheme to defraud the CAC / NEPA.

Saar diverted fraudulent payments of various kinds from CAC / NEPA bank accounts into her own personal bank accounts for her personal benefit. Some of the diverted payments involved fraudulent mileage reimbursements, while others involved Saar inflating her bi-weekly paychecks by thousands of dollars. The total amount of fraudulent diversions as alleged in the criminal information is $411,940.11. (Source)

Company Accounting Controller Sentenced To Prison For Stealing $262,000+ - July 22, 2024

Amy Hall was sentenced to 3 years in prison, followed by 3 years of supervised release, for seven counts of wire fraud. The charges in this case stemmed from Hall's scheme in which, while employed as the Accounting Controller for a Louisville, Kentucky design and construction company, she used her access and position to make unauthorized payments totaling $262,897.69, for her own personal benefit and the benefit of others, on the company's bank account, a related company's bank account, and a company credit card without the companies' knowledge or authorization. (Source)

Hall was also ordered to pay restitution to the two victim companies in the amount of $262,897.69. (Source)

Former Employee Sentenced To Prison For Robbing Food Lion - July 22, 2024

Christopher Harris, is a former Food Lion employee. He pulled a gun on a Food Lion cashier and robbed the store.

On June 28, 2023, Harris entered the Food Lion grocery store where he used to be employed, placed two bags of Cheetos on the counter, and gave the cashier a $1 bill and some change. When the cashier opened the register, Harris pulled out a firearm, pointed it at the cashier, and twice told the cashier to "back the fu*k up."

The cashier put his hands up and backed away from the register while Harris grabbed the entire cash drawer and ran out with the contents, approximately $1,217.

On July 6, 2023, law enforcement arrested Harris who confessed to robbing the store and described where he had abandoned the cash drawer, which was later recovered. (Source)

CEO Of Publicly Traded Company Convicted For Role In Securities Fraud Scheme Involving COVID Test Kits - July 10, 2024

Marc Schessel is the former CEO of SCWorx Corp. (SCWorx), which is publicly traded health care company. He was convicted for his role in a scheme to mislead investors about SCWorx's procurement of COVID-19 rapid test kits in the early days of the COVID-19 pandemic.

Schessel caused SCWorx to issue multiple public statements claiming that SCWorx was buying and reselling at least 48 million COVID-19 test kits, despite knowing that such statements were false and misleading. , Schessel made, or caused to be issued, four false and misleading statements during a five-day period in April 2020.

All four announcements claimed that SCWorx would be receiving millions of COVID-19 rapid test kits within two weeks, but Schessel and SCWorx never acquired a single COVID-19 test kit as part of the announced transaction.

In the wake of these public announcements, SCWorx's share price surged, rising by over 400%, from approximately $2.25 to an intraday high of $14.88. After SCWorx announced that it was terminating these COVID-19 rapid test kit agreements without having acquired any tests, SCWorx's share price quickly dropped below its pre-April 13, 2020 announcement price. (Source)

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

Vice President Of Miami Aerospace Company & Accomplice Sentenced To Prison For Embezzling $2.1 Million+ Over 10 Years / Used Funds To Pay For Family Expenses - July 8, 2024

From August 2008, and continuing through October 2018, Mario La Torre used his position as Senior Vice President of Sales and Marketing for Miami-based Summit Aerospace, Inc. (Summit), to fraudulently embezzle over $2.1 million of Summit's funds, which he split with his co-defendant, Joe McHomes. La Torre evaded the payment of income tax on his ill-gotten gains, by laundering the fraud proceeds and filing false and fraudulent income tax returns.

La Torre used the fraud proceeds to pay family expenses, including, among other things, his wife's credit card bills and his daughter's university education. (Source)

Manager Of Hilton Sentenced To Prison For Receiving $1.6 Million+ In Kickbacks For $6.4 Million+ Of Construction & Renovation Work - July 12, 2024

From 2008 through 2016 Geoffrey, Palermo was working as the manager of the Hilton hotel located in downtown San Francisco. During this timeframe, Palermo had authority to enter into contracts, choose contractors, and otherwise manage construction and capital improvement projects at the hotel.

Palermo admitted he devised a kickback scheme involving contractors to deprive the Hilton hotel's owners of more than $1.8 million in kickbacks that went to Palermo.

As part of the scheme, Palermo agreed with one contractor, Adan Roldan, that Roldan would submit falsely inflated invoices for construction and renovation work at the hotel, that Palermo would approve the false invoices, and that Roldan and the second contractor would pay a kickback to Palermo associated with the falsely inflated invoices.

From 2013 through 2016, as a result of this scheme, Palermo approved and the hotel's owners paid over $6.4 million to Roldan Construction based on invoices submitted by Roldan's construction company. In exchange, Roldan paid more than $1.6 million in kickbacks to Palermo.

Additionally, in 2014 and 2015, Palermo approved and the hotel's owners paid over $2 million to a second contractor based on falsely inflated invoices submitted by that contractor, and the contractor paid Palermo over $300,000 in kickbacks. In exchange for kickbacks, Palermo continued to hire Roldan and the second contractor to do work at the Hilton. (Source)

Law Firm Chief Financial Officer Charged With Embezzling $1.2 Million+ / Used Funds To Purchase 3 Homes - July 1, 2024

Tony Archuleta-Perkins started a non-profit organization called Murrieta Valley High School 1994 (MVHS 1994), in 2013.

From 2017 to 2023, Archuleta-Perkins worked for two San Francisco law firms. He held various roles at the firms, eventually becoming Chief Financial Officer (CFO).

From May 2018 through December 2023, Archuleta-Perkins caused the law firms to make false and fraudulent payments to MVHS 1994 that had not been authorized by the law firms' management and were not for any legitimate business purpose.

Once the stolen funds were in MVHS 1994's bank account, Archuleta-Perkins would sometimes directly issue payments to vendors and accounts for personal expenses that had nothing to do with the stated purposes of MVHS 1994 or the law firms. On other occasions, he wrote checks from MVHS 1994 to himself and deposited those checks into his personal bank account.

Archuleta-Perkins falsely endorsed a $41,663.69 U.S. Treasury check made out to one of the law firms, deposited it into a bank account belonging to MVHS 1994 and then wrote himself a check for the same amount.

Archuleta-Perkins used the stolen money for personal expenses, including payments on Best Buy and Home Depot credit cards, and towards the purchase, renovation, and improvement of at least three properties in California. (Source)

Family Crisis & Counseling Center Manager Sentenced To Prison For Embezzling $278,000+ / Used Funds For Gambling Addiction - July 25, 2024

In 2012, the Family Crisis and Counseling Center (FCCC) in Bartlesville, Oklahoma hired Deanna Long as a manager. She was entrusted to handle many aspects of FCCC's accounting and finance functions, including record-keeping for the financial books, paying bills, and preparing checks for business expenses.

Within two years of being hired, Long began embezzling money to fund personal expenses and fuel her gambling addiction. Long embezzled more than $278,000 from FCCC.

Long was orderd to pay $278,257.54 in restitution.

State court records show Long has been arrested numerous times for passing bogus checks, pled guilty to bogus check charges, and pled guilty twice for embezzling from two prior employers. (Source)

Executive Director For Charity Sentenced To Prison For Embezzling $240,000 / Used Funds For Gambling - July 24, 2024

Kyle Fisher was the Executive Director of LISTEN Community Services from approximately August 2016 - October 2022. As Executive Director, Fisher had full access to LISTEN's finances, including its bank account and PayPal account, which it used to collect donations. Fisher made unauthorized transfers from LISTEN's bank accounts and PayPal to accounts he controlled. He also wrote eight unauthorized checks payable to himself. Fisher then spent the stolen funds on personal expenses, primarily gambling at a casino in Springfield, Massachusetts.

For example, on January 24, 2022, Fisher withdrew $4,787 from LISTEN's PayPal account and transferred the funds to his personal bank account. Later that same day, Fisher made multiple withdrawals from his bank account, including at ATMs at the casino. He then deposited a substantial amount of cash into his personal casino account that day. The casino records showed that Fisher continuously gambled on January 24, 2022 and January 25, 2022, and lost a combined $6,719 over those two days.

Fisher also took steps to conceal his embezzlement from LISTEN. For example, he created a fake PayPal statement that showed over $94,000 in payments to Dell. Fisher also provided fraudulent invoices to LISTEN.

In total Fisher embezzled almost $240,000 from LISTEN. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Company Operations Manager Pleads Guilty To Embezzling $1.49 Million+ Over 7 Years Using Fake Invoice Scheme / Used Funds For Mortgage Payments, Car Loans, Vacation, Etc. - July 18, 2024

From 2004 to 2020, Gabriel De Chavez worked as an Operations Manager.

Between 2012 and 2019, De Chavez used his position to generate fake invoices purportedly created by genuine vendors for goods and services. He presented these fake invoices and corresponding checks made out to the real vendors to his employer for signature, and would then deposit the checks into his own personal bank account.

De Chavez used the funds to pay for personal expenses including credit card payments, cash withdrawals, mortgage payments, vacations, and car loans. He was able to continue the scheme without notice because of the trusted position he held at the company. Between 2012 and 2019, Ruiz De Chavez created over 600 fake invoices and checks, causing at least $1,491,000 to be transferred into his account from his employer.
(Source)

NETWORK / IT SABOTAGE / OTHER FORMS OF SABOTAGE / UN-AUTHORIZED ACCESS TO COMPUTER SYSTEMS & NETWORKS
No Incidents To Report

THEFT OF ORGANIZATIONS ASSESTS
No Incidents To Report

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)
No Incidents To Report

EMPLOYEE DRUG RELATED INCIDENTS
No Incidents To Report

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 FRAUD

Former Wells Fargo Executive Pleads Guilty To Opening Millions Of Accounts Without Customer Authorization - Wells Fargo Agrees To Pay $3 BILLION Penalty - March 15, 2023

The former head of Wells Fargo Bank's retail banking division (Carrie Tolstedt) has agreed to plead guilty to obstructing a government examination into the bank's widespread sales practices misconduct, which included opening millions of unauthorized accounts and other products.

Wells Fargo in 2020 acknowledged the widespread sales practices misconduct within the Community Bank and paid a $3 BILLION penalty in connection with agreements reached with the United States Attorneys' Offices for the Central District of California and the Western District of North Carolina, the Justice Department's Civil Division, and the Securities and Exchange Commission.

Wells Fargo previously admitted that, from 2002 to 2016, excessive sales goals led Community Bank employees to open millions of accounts and other financial products that were unauthorized or fraudulent. In the process, Wells Fargo collected millions of dollars in fees and interest to which it was not entitled, harmed customers' credit ratings, and unlawfully misused customers' sensitive personal information.

Many of these practices were referred to within Wells Fargo as "gaming." Gaming strategies included using existing customers' identities – without their consent – to open accounts. Gaming practices included forging customer signatures to open accounts without authorization, creating PINs to activate unauthorized debit cards, and moving money from millions of customer accounts to unauthorized accounts in a practice known internally as "simulated funding." (Source)

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

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

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

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

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

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

Former Goldman Sachs (GS) Managing Director Sentenced To Prison For Paying $1.6 BILLION In Bribes To Malaysian Government Officials To Launder $2.7 BILLION+ Embezzled From Malaysia Development Company / GS Agrees To Pay Over $2.9 BILLION Criminal Penalty - March 9, 2023

Ng Chong Hwa, also known as "Roger Ng," a citizen of Malaysia and a former Managing Director of The Goldman Sachs Group, Inc., was was sentenced to 10 years in prisont for conspiring to launder BILLIONS of dollars embezzled from 1Malaysia Development Berhad (1MDB), conspiring to violate the Foreign Corrupt Practices Act (FCPA) by paying more than $1.6 BILLION in bribes to a dozen government officials in Malaysia and Abu Dhabi, and conspiring to violate the FCPA by circumventing the internal accounting controls of Goldman Sachs.

1MDB is a Malaysian state-owned and controlled fund created to pursue investment and development projects for the economic benefit of Malaysia and its people.

Between approximately 2009 and 2014, Ng conspired with others to launder billions of dollars misappropriated and fraudulently diverted from 1MDB, including funds 1MDB raised in 2012 and 2013 through three bond transactions it executed with Goldman Sachs, known as "Project Magnolia," "Project Maximus," and "Project Catalyze." As part of the scheme, Ng and others, including Tim Leissner, the former Southeast Asia Chairman and participating managing director of Goldman Sachs, and co-defendant Low Taek Jho, a wealthy Malaysian socialite also known as "Jho Low," conspired to pay more than a billion dollars in bribes to a dozen government officials in Malaysia and Abu Dhabi to obtain and retain lucrative business for Goldman Sachs, including the 2012 and 2013 bond deals.

They also conspired to launder the proceeds of their criminal conduct through the U.S. financial system by funding major Hollywood films such as "The Wolf of Wall Street," and purchasing, among other things, artwork from New York-based Christie's auction house including a $51 million Jean-Michael Basquiat painting, a $23 million diamond necklace, millions of dollars in Hermes handbags from a dealer based on Long Island, and luxury real estate in Manhattan.

In total, Ng and the other co-conspirators misappropriated more than $2.7 billion from 1MDB.

Goldman Sachs also paid more than $2.9 billion as part of a coordinated resolution with criminal and civil authorities in the United States, the United Kingdom, Singapore, and elsewhere. (Source)

Boeing Charged With 737 Max Fraud Conspiracy Agrees To Pay Over $2.5 BILLION In Penalties Because Of Employees Fraudulent And Deceptive Conduct - January 11, 2021

Aircraft manufacturer Boeing has agreed to pay over $2.5 billion in penalties as a result of "fraudulent and deceptive conduct by employees" in connection with the firm's B737 Max aircraft crashes.

"The misleading statements, half-truths, and omissions communicated by Boeing employees to the FAA impeded the government's ability to ensure the safety of the flying public," said U.S. Attorney Erin Nealy Cox for the Northern District of Texas.

As Boeing admitted in court documents, Boeing through two of its 737 MAX Flight Technical Pilots deceived the FAA about an important aircraft part called the Maneuvering Characteristics Augmentation System (MCAS) that impacted the flight control system of the Boeing 737 MAX. Because of their deception, a key document published by the FAA lacked information about MCAS, and in turn, airplane manuals and pilot-training materials for U.S.-based airlines lacked information about MCAS.

On Oct. 29, 2018, Lion Air Flight 610, a Boeing 737 MAX, crashed shortly after takeoff into the Java Sea near Indonesia. All 189 passengers and crew on board died.

On March 10, 2019, Ethiopian Airlines Flight 302, a Boeing 737 MAX, crashed shortly after takeoff near Ejere, Ethiopia. All 157 passengers and crew on board died. (Source)

2 Former Employees Of Mortgage Lending Business Charged For Roles In $1.4 BILLION+ Mortgage Loan Fraud Scheme – April 24, 2024

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)

Member Of Supervisory Board Of State Employees Federal Credit Union Pleads Guilty To $1 BILLION Scheme Involving High Risk Cash Transactions - January 31, 2024

A New York man pleaded guilty today to failure to maintain an anti-money laundering program in violation of the Bank Secrecy Act as part of a scheme to bring lucrative and high-risk international financial business to a small, unsophisticated credit union.

From 2014 to 2016, Gyanendra Asre of New York, was a member of the supervisory board of the New York State Employees Federal Credit Union (NYSEFCU), a financial institution that was required to have an anti-money laundering program. Through the NYSEFCU and other entities, Asre participated in a scheme that brought over $1 billion in high-risk transactions, including millions of dollars of bulk cash transactions from a foreign bank, to the NYSEFCU.

In addition, Asre was a certified anti-money laundering specialist who was experienced in international banking and trained in anti-money laundering compliance and procedures, and represented to the NYSEFCU that he and his businesses would conduct appropriate anti-money laundering oversight as required by the Bank Secrecy Act. Based on Asre's representations, the NYSEFCU, a small credit union with a volunteer board that primarily served New York state public employees, allowed Asre and his entities to conduct high-risk transactions through the NYSEFCU. Contrary to his representations, Asre willfully failed to implement and maintain an anti-money laundering program at the NYSEFCU. This failure caused the NYSEFCU to process the high-risk transactions without appropriate oversight and without ever filing a single Suspicious Activity Report, as required by law. (Source)

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

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

The Justice Department today announced the 2024 National Health Care Fraud Enforcement Action, which resulted in criminal charges against 193 defendants, including 76 doctors, nurse practitioners, and other licensed medical professionals in 32 federal districts across the United States, for their alleged participation in various health care fraud schemes involving approximately $2.75 billion in intended losses and $1.6 billion in actual losses.

In connection with the coordinated nationwide law enforcement action, and together with federal and state law enforcement partners, the government seized over $231 million in cash, luxury vehicles, gold, and other assets.

The charges alleged include over $900 million fraud scheme committed in connection with amniotic wound grafts; the unlawful distribution of millions of pills of Adderall and other stimulants by five defendants associated with a digital technology company; an over $90 million fraud committed by corporate executives distributing adulterated and misbranded HIV medication; over $146 million in fraudulent addiction treatment schemes; over $1.1 billion in telemedicine and laboratory fraud; and over $450 million in other health care fraud and opioid schemes. (Source)

2 Executives Who Worked For a Geneva Oil Production Firm Involved In Misappropriating $1.8 BILLION - April 25, 2023

The former Petrosaudi employees are suspected of having worked with Jho Low, the alleged mastermind behind the scheme, to set up a fraudulent deal purported between the governments of Saudi Arabia and Malaysia, according to a statement from the Swiss Attorney General.

1MDB was the Malaysian sovereign wealth fund designed to finance economic development projects across the southeastern Asian nation but become a byword for scandal and corruption that triggered investigations in the US, UK, Singapore, Malaysia, Switzerland and Canada.

Low, currently a fugitive whose whereabouts are unknown, has previously denied wrongdoing. His playboy lifestyle was financed with money stolen from 1MDB, according to US prosecutors.

The pair are accused of having used the facade of a joint-venture and $2.7 billion in assets "which in reality it did not possess" to lure $1 billion in financing from 1MDB, according to Swiss prosecutors. The two opened Swiss bank accounts to receive the money, and then used the proceeds to acquire luxury properties in London and Switzerland, as well as jewellery and funds "to maintain a lavish lifestyle," the prosecutors said.

The allegations cover a period at least from 2009 to 2015 and the duo have been indicted for commercial fraud, aggravated criminal mismanagement and aggravated money laundering. (Source)

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)

CEO, Vice President Of Business Development And 78 Individuals Charged In $2.5 BILLION in Health Care Fraud Scheme - June 28, 2023

The Justice Department, together with federal and state law enforcement partners, announced today a strategically coordinated, two-week nationwide law enforcement action that resulted in criminal charges against 78 defendants for their alleged participation in health care fraud and opioid abuse schemes that included over $2.5 Billion in alleged fraud. The enforcement action included charges against 11 defendants in connection with the submission of over $2 Billion in fraudulent claims resulting from telemedicine schemes.

In a case involving the alleged organizers of one of the largest health care fraud schemes ever prosecuted, an indictment in the Southern District of Florida alleges that the Chief Executive Officer (CEO), former CEO, and Vice President of Business Development of purported software and services companies conspired to generate and sell templated doctors' orders for orthotic braces and pain creams in exchange for kickbacks and bribes. The conspiracy allegedly resulted in the submission of $1.9 Billion in false and fraudulent claims to Medicare and other government insurers for orthotic braces, prescription skin creams, and other items that were medically unnecessary and ineligible for Medicare reimbursement. (Source)

10 Individuals (Hospital Managers And Others) Charged In $1.4 BILLION Hospital Pass - Through Billing Scheme - June 29, 2020

10 individuals, including hospital managers, laboratory owners, billers and recruiters, were charged for their participation in an elaborate pass-through billing scheme using rural hospitals in several states as billing shells to submit fraudulent claims for laboratory testing.

The indictment alleges that from approximately November 2015 through February 2018, the conspirators billed private insurance companies approximately $1.4 billion for laboratory testing claims as part of this fraudulent scheme, and were paid approximately $400 million. (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)

TRADE SECRET THEFT

Former Scientist Convicted For Role With Sister To Steal Trade Secrets From GlaxoSmithKline Worth $10 BILLION - May 2, 2022

Gongda Xue worked as a scientist at the Friedrich Miescher Institute for Biomedical Research (FMI) in Switzerland, which is affiliated with Novartis. His sister, Yu Xue, worked as a scientist at GlaxoSmithKline (GSK) in Pennsylvania. Both Gongda Xue and Yu Xue conducted cancer research as part of their employment at these companies.

While working for their respective entities, Gongda Xue and Yu Xue shared confidential information for their own personal benefit.

Gongda Xue created Abba Therapeutics AG in Switzerland, and Yu Xue and her associates formed Renopharma, Ltd., in China. Both companies intended to develop their own biopharmaceutical anti-cancer products.

Gongda Xue stole FMI research into anti-cancer products and sent that research to Yu Xue. Yu Xue, in turn, stole GSK research into anti-cancer products and sent that to Gongda Xue. Yu Xue also provided hundreds of GSK documents to her associates at Renopharma. Renopharma then attempted to re-brand GSK products under development as Renopharma products and attempted to sell them for billions of dollars. Renopharma's own internal projections showed that the company could be worth as much as $10 billion based upon the stolen GSK data. (Source)

U.S. Brokerage Firm Accuses Rival Firm Of Stealing Trade Secrets Valued At Over $1 BILLION - November 14, 2023

U.S. brokerage firm BTIG sued rival StoneX Group, accusing it of stealing trade secrets and seeking at least $200 million in damages.

StoneX recruited a team of BTIG traders and software engineers to exfiltrate BTIG software code and proprietary information and take it to StoneX, according to lawyers for BTIG.

StoneX used the software code and proprietary information to build competing products and business lines that generate tens of millions of dollars annually, they alleged in the lawsuit.

BTIG said in the lawsuit that StoneX had committed one of the greatest financial industry trade secret frauds in recent history, and that the scope of its misconduct is not presently known, and may easily exceed a billion dollars."

The complaint said StoneX hired several BTIG employees to steal confidential information that it used to develop its competing trading platform.

The complaint said that StoneX's stock price has increased 60% since it started misusing BTIG's trade secrets. (Source)

U.S. Petroleum Company Scientist Sentenced To Prison For $1 BILLION Theft Of Trade Secrets - Was Starting New Job In China - May 27, 2020

When scientist Hongjin Tan resigned from the petroleum company he had worked at for 18 months, he told his superiors that he planned to return to China to care for his aging parents. He also reported that he hadn't arranged his next job, so the company agreed to let him to stay in his role until his departure date in December 2018.

But Tan told a colleague a different story over dinner. He revealed to his colleague that he actually did have a job waiting for him in China. Tan's dinner companion reported the conversation to his supervisor. That conversation prompted Tan's employer to ask him to leave the firm immediately, and his employer made a call to the FBI tip line to report a possible crime.

Tan called his supervisor to tell them he had a thumb drive with company documents on it. The company told him to return the thumb drive. When he brought back the thumb drive, the company looked at the slack space on the drive and found several files had been erased. The deleted files were the files the company was most concerned about. (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 Role in $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)

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)

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 (**5,500+ Incidents**).

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

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

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

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

INSIDER THREAT INCIDENTS SPOTLIGHT REPORT FOR 2023

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

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

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

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

Incident Posting Notifications

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

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

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

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER

Updated Daily

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

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

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

National Insider Threat Special Interest Group (NITSIG)

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

NITSIG Overview

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

NITSIG Membership

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

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

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

NITSIG Meetings

The NITSIG provides education and guidance to the membership via in person meetings, webinars and other events, that is practical, strategic, operational and tactical in nature. Many members have even stated the NITSIG is like having a team of IRM experts at their disposal FREE OF CHARGE. The NITSIG has meetings primarily held at the John Hopkins University Applied Physics Lab in Laurel, Maryland and other locations (NITSIG Chapters, Sponsors). There is **NO CHARGE** to attend. See the link below for some of the great speakers we have had at our meetings.
http://www.nationalinsiderthreatsig.org/nitsigmeetings.html

NITSIG IRM Resources

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

NITSIG LinkedIn Group

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

NITSIG Insider Threat Symposium & Expo

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

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

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

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

NITSIG Advisory Board

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

INSIDER THREAT DEFENSE GROUP

Insider Risk Management Program Experts

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

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

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

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

INSIDER RISK MANAGEMENT (IRM) PROGRAM CONSULTING SERVICES OFFERED

Conducted Via Classroom / Onsite / Web Based

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

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

White House, U.S. Government Agencies, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines), Intelligence Community Agencies (DIA, NSA, NGA), Law Enforcement (DHS, TSA, FBI, U.S. Secret Service, DEA, Police Departments), Critical Infrastructure Providers, Universities, Fortune 100 / 500 companies and others; Microsoft, Verzion, Walmart, Home Depot, Nike, Tesla, Dell Technologies, Nationwide Insurance, Discovery Channel, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more. The ITDG has provided training and consulting services to over **675+** organizations. (Client Listing)

Additional Background Information On ITDG

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

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

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

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

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

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