INSIDER THREAT INCIDENTS REPORT
FOR
March 2025

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

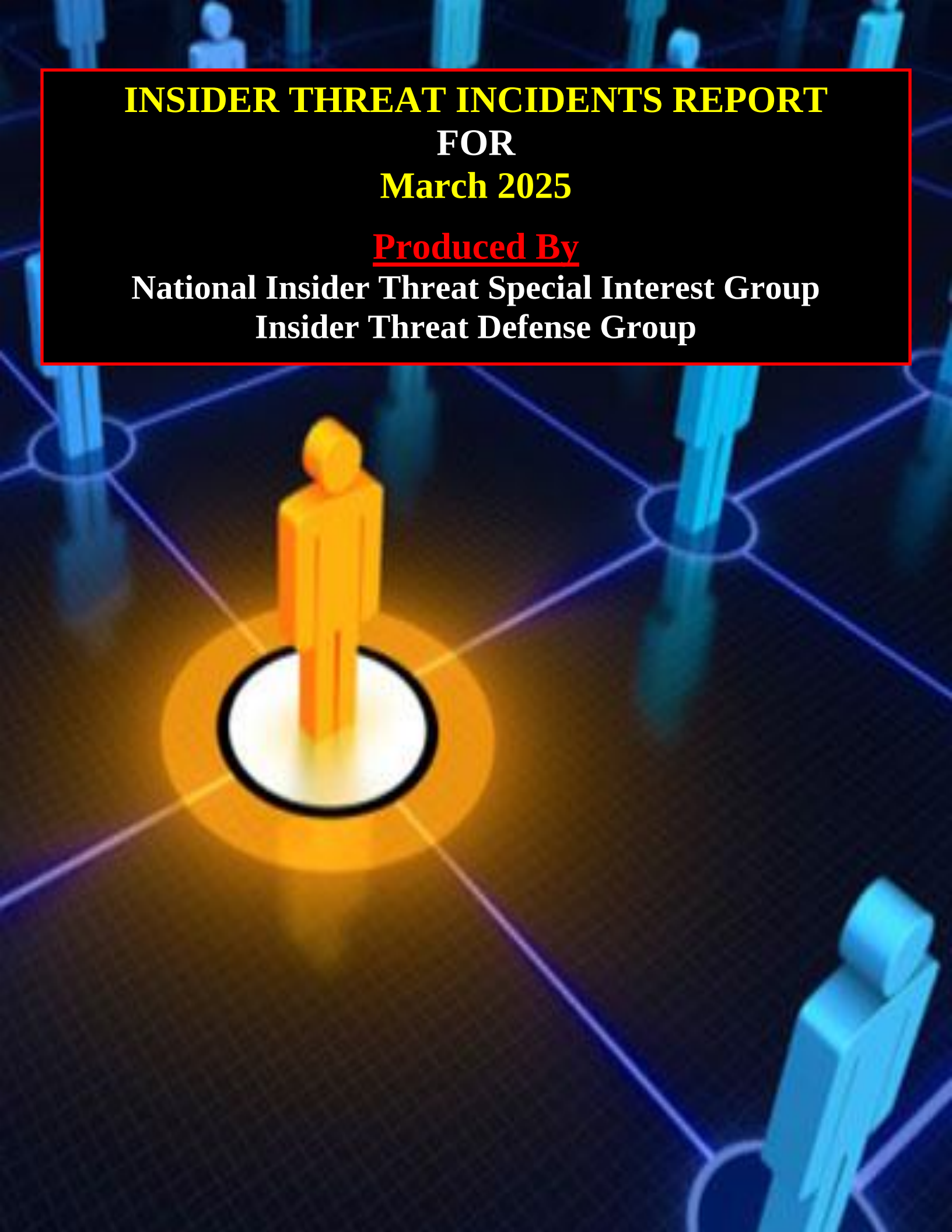


TABLE OF CONTENTS

INSIDER THREAT INCIDENTS

A Very Costly And Damaging Problem

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

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for 15+ years. This research has evaluated and analyzed over **6,100+** 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. **Companies have also had large layoffs or gone out of business because of the malicious actions of employees.**

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 MARCH 2025

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

Korea Aerospace Research Institute Employees Under Investigation For Leaking Sensitive Rocket Technology - March 18, 2025

An employee of the Korea Aerospace Research Institute (KARI) is currently under investigation by the Daejeon Metropolitan Police Agency for allegedly leaking sensitive rocket technology. The investigation, which has captured national attention, involves a suspected breach of data related to South Korea's ambitious Nuri space launch vehicle project. Police conducted a search and seizure operation at the office of the implicated employee, identified as A, who is suspected of violating the Unfair Competition Prevention Act among other charges.

The investigation stems from a report made by KARI late last year, after researchers at the Launch Vehicle Research Center detected a significant data breach. The breach involved the unauthorized export of data that was meant to be confined within KARI's internal network. This incident has raised serious concerns about data security within the institute, which plays a pivotal role in South Korea's space exploration and satellite development efforts.

Employee A is not the only individual under scrutiny. Colleague B, who has since resigned and joined a private company, is also being investigated. Evidence has surfaced suggesting that A and B exchanged sensitive data via messenger, further complicating the case.

The Nuri project, also known as KSLV-II, is a cornerstone of South Korea's efforts to establish itself as a formidable player in the global space industry. Given the strategic importance of such technology, any leak could have significant national security implications and affect the country's international competitiveness.

In October 2023, KARI faced allegations of technology leaks involving employees who were about to resign. Although four employees were referred to prosecution following an audit by the Ministry of Science and ICT, no charges were filed. This backdrop underscores ongoing challenges KARI faces in safeguarding its technological assets. (Source)

U.S. GOVERNMENT

U.S Postal Worker Found Guilty Of Stealing $1.6 Million+ In Checks From U.S. Mail / Used Funds For International Travel, Etc. - March 14, 2025

Between December 2020 and March 2023, Hachikosela Muchimba was an employee of the U.S. Postal Service when he executed a scheme to steal U.S. Treasury checks and private party checks from the U.S. mail.

Muchimba then deposited the checks, which he either altered and/or falsely endorsed, into bank accounts under his control. Muchimba altered some of the checks by removing the name of the proper payee on the checks and replacing it with his own name. Bank surveillance footage captured images of him making deposits and withdrawals of the funds. The total amount of the U.S. Treasury checks fraudulently deposited into Muchimba's various bank accounts was just over $1.6 million.

Muchimba used the proceeds of the stolen checks to fund a lavish lifestyle that included international travel, stays at luxury hotels, and purchases at gentlemen's clubs. (Source)

Former U.S. Postal Service Employee Pleads Guilty To Stealing $18,000 Of Postal Orders - March 27, 2025

Christine Hedges began working for USPS around 2020, most recently as a Lead Sales & Service Associate in Brockton, Massachusetts.

From approximately October 2021 to August 2023, Hedges engaged in a scheme to steal USPS funds for her personal use. As part of this scheme, Hedges generated, for her own use, no-fee money orders without a customer physically present at her customer window and which a customer did not request. Hedges also stole cash from her USPS workstation and often attempted to conceal her theft by replacing the cash with these fraudulent money orders.

During the relevant period, Hedges generated approximately 64 fraudulent no-fee money orders. Of those no-fee money orders, 11 were made out to her boyfriend or a family member. From on or about Aug. 1, 2023 to on or about Aug. 14, 2023, video surveillance from above Hedges' workstation showed Hedges on at least one occasion removing cash from her assigned drawer and putting it in her pocket. In all, Hedges stole approximately $18,939 in postal funds. (Source)

U.S. Postal Service Employee Pleads Guilty To Stealing $17,000+ - March 27, 2025

According to court records, in October 2022, U.S. Postal Service Office of Inspector General (USPS-OIG) launched an investigation after receiving a report that postal funds were missing following stamp stock and cash counts at the Cherryfield Post Office in Maine.

Surveillance video from within the post office captured Melissa Milliken placing money into her pockets. Milliken admitted to investigators that she had been stealing from the post office for approximately a year. Investigators determined she stole more than $17,130 in government money between December 2021 and September 2023. (Source)

U.S. Postal Worker Charged With Accepting Bribes To Facilitate The Shipment Of Drug Filled Parcels - March 28, 2025

From 2022 to 2023 Keith Toney received bribes to facilitate the shipment of drug-filled parcels by coordinating with a drug-distributor to arrange for the delivery of drug-filled parcels, and personally delivering and turning over the drug-filled parcels to a drug-distributor. (Source)

Department Of State Employee Charged For The Unauthorized Release Of Classified Information To Individuals He Met Online - March 7, 2025

Michae Schena is employed by the U.S. Department of State (DOS) working out of DOS Headquarters in Washington, D.C. Schena held a top secret security clearance and had access to information up to the secret level within his DOS workspace.

Beginning in or about April 2022, Schena allegedly communicated with people he met online through various communication platforms and provided them with information they were not authorized to receive. In return, Schena received payments.

On Feb. 27, Schena allegedly used a cellphone to take images of multiple documents, which were displayed on the monitor of his classified computer and marked as "SECRET." Schena then allegedly left work and returned to his home in Alexandria, where the cellphone was seized. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

4 U.S. Army Soldiers Sentenced To Prison For Stealing $2.7 Million Of Items From Fort Cavazos In Texas - March 27, 2025

Beginning in January 2017, Benjamin Alvarado Jr., 32, purchased thousands of military items, owned by the United States, from co-conspirators Darius Alston, Justin Wallas and Gabriel Taylor, and Kynyqus Bryant.
The co-conspirators were U.S. Army soldiers stationed at Fort Cavazos in Texas and had participated in at least seven thefts of U.S. government property from Fort Cavazos. Collectively, they coordinated with Alvarado throughout the scheme through telecommunications and text messages.

Investigators with the Department of the Army Criminal Investigation Division (Army CID) traced several transactions through online sellers, such as eBay, to Alvarado, who, on Aug, 9, 2021, was discovered to be selling multiple M-50 gas masks similar to what had been reported stolen from Fort Cavazos. Alvarado was also selling filters for the masks, night vision device image intensifier tubes, Litefighter tents, and other miscellaneous sensitive property being transported in interstate and foreign commerce with a value of $5,000 or more

Executed search warrants resulted in the recovery of more than 24,000 individual items stolen from the U.S. government, including, in addition to the items previously named, weapons parts, and Level III and Level IV body armor. The recovered properties were valued at approximately $2.75 million. Another search warrant led to the recovery of another $100,000 worth of military property at a Killeen storage building. The investigation also revealed that, on or about Jan. 5, 2021, Alvarado participated in the sale and transfer of a Joint Chemical Agent Detector M4A1 to a buyer in China through an intermediary in Delaware.

Alvarado stated he had purchased 90% of the 24,000 items seized from Bryant and Alston, who were assigned to the 553rd Combat Service Support Battalion. Taylor later confessed that he had participated as the lookout in a July 2021 robbery on Fort Cavazos, while other members of the conspiracy retrieved the items. Alston stated that he had conducted seven or eight theft operations with Bryant and the others, also as a lookout.

On Sept. 3, 2019, Alvarado transferred a cashier's check for $52,890.55 to a title company for a residence in Killeen. On July 7, 2021, Alvarado transferred a personal check for $50,000 to a licensed automobile dealer for the purchase of a 2013 McLaren MP4. Following the April 2022 indictment, Alvarado forfeited the house and the car. (Source)

2 Veterans Affairs Medical Center Employees Plead Guilty To Each Accepting $16,000+ In Bribes From Sales Representatives - March 27, 2025

Monika Schorer and Teresa Schorer entered guilty pleas to conspiracy to commit honest services wire fraud.

Each woman worked for the James H. Quillen VA Medical Center in Mountain Home, Tennessee, and each accepted cash bribe payments from individuals who worked as a surgical sales representative for an independent distributor of a nationwide orthopedic company that manufactured replacement joints and products used during surgeries in which those joints were implanted. The sales representatives routinely sold products to the VA Medical Center where the women worked. According to the filed plea agreements, the sales representatives (who have previously entered guilty pleas) formed a separate company in June 2018 and began selling their own acquired inventory to the VA at inflated prices or when not medically necessary, resulting in losses to the VA. By their written plea agreements, each defendant agreed that they conspired and accepted cash bribe payments from the sales representatives of $9,900 each in September 2018 and $7,000 each in October 2018 for their agreement to commit, collude, and aid in the fraud against the VA. (Source)

Active-Duty And Former U.S. Army Soldiers Arrested For Theft Of Classified Information & Bribery Scheme - March 6, 2025

Jian Zhao, and Li Tian, active-duty U.S. Army soldiers stationed at Joint Base Lewis-McChord, along with Ruoyu Duan, a former U.S. Army soldier, were arrested.

From November. 28, 2021, and continuing to at least on or about Dec. 19, 2024, Duan and Tian along with others, known and unknown to the grand jury conspired with each other to surreptitiously gather sensitive military information related to the United States Army's operational capabilities, including technical manuals and other sensitive information, and that Tian transmitted this information to Duan in return for money. Specifically, Tian was tasked with gathering information related U.S. military weapon systems, including information related to the Bradley and Stryker U.S. Army fighting vehicles, and transmitting them to Duan.

From about July 2024, and continuing to the date of the arrest, Jian Zhao, an active-duty U.S. Army Supply Sergeant, conspired with others known and unknown to the grand jury to obtain and transmit national defense information to individuals based in China. Zhao is further alleged to have committed bribery and theft of government property.

Specifically, Zhao was charged for his conspiracy to collect and transmit several classified hard drives, including hard drives marked "SECRET" and "TOP SECRET", negotiating with individuals based in China for their sale, and agreeing to send the classified hard drives to the individuals in China. In exchange for the sale of the classified hard drives, Zhao received at least $10,000. Zhao is further alleged to have conspired to sell an encryption capable computer that was stolen from the U.S. Government, and sensitive U.S. military documents and information, including information related to the High Mobility Artillery Rocket System (HIMARS), and information related to U.S. military readiness in the event of a conflict with the People's Republic of China.

Zhao is alleged to have violated his duties as a U.S. Army Soldier and public official to protect sensitive military information in exchange for money. In total, Zhao is alleged to have corruptly received and accepted payments totaling at least $15,000. (Source)

Department Of Defense Employee Pleads Guilty To Unauthorized Removal & Retention Of Classified Information - March 20, 2024

Gokhan Gun was a civilian electrical engineer for the Department of Defense. He has pleaded guilty to unauthorized removal and retention of classified material.

Gun, 51, of Falls Church, Virginia, was born in Istanbul, Turkey, and is a dual citizen of Turkey and the United States. Through his employment, Gun possessed a Top Secret security clearance with access to Sensitive Compartmented Information (SCI) and received training on the proper handling and storage of classified information.

Beginning in May 2024, Gun, without permission, removed at least five classified documents from his Department of Defense workspace with the intent to retain them at his primary residence, which was not an approved facility for the storage of classified information.

On Aug. 9, 2024, Gun was scheduled to depart the United States on a morning flight to Mexico. However, FBI agents observed a ride share service arrive at the defendant's residence and approached Gun. Agents observed inside Gun's residence a backpack inside which they located a Top Secret document and a notebook with handwritten notes that mirrored a Top Secret report. In the dining room, agents located additional classified documents, one of which Gun printed on Aug. 7, 2024, just two days before his scheduled departure. (Source)

U.S. Naval Reservist Charged With Paying Bribe To Obtain DoD Identification Cards For Unauthorized Individuals, Including A Chinese National - March 3, 2025

In January 2025, a confidential source reported to law enforcement that Raymond Zumba who serves in the U.S. Navy Reserve, was aware that the source's spouse worked at Naval Air Station (NAS) Jacksonville in the personnel office that issues Department of Defense identification cards. The source reported that Zumba asked whether the spouse would be willing to issue real, but unauthorized identification cards for an under-the-table payment. Acting at the direction of federal agents, the source proceeded to engaged in a series of communications with Zumba during which they discussed Zumba's plan to obtain unauthorized ID cards in exchange for cash.

After driving from New York, Zumba arrived in Jacksonville on February 13, 2025, with three individuals, including a Chinese national. Zumba brought these individuals to NAS Jacksonville where the source's spouse let them into the personnel office after business hours and initiated the process for two of them to receive ID cards. The following day, Zumba met with the source, who gave him two cards in exchange for $3,500. Zumba was promptly arrested, and the cards were recovered. (Source)

Department of Defense Employee Sentenced To Prison The Unauthorized Removal / Retention of Classified Documents - March 26, 2025

Margaret Ashby, 26, was sentenced to 36 months in prison and a fine of $15,000 after pleading guilty to Unauthorized Removal/Retention of Classified Documents.

Ashby was hired in March 2020 as a civilian employee of a Department of Defense component agency located in the Southern District of Georgia. As required for her employment, Ashby possessed a Top Secret security clearance.

From February 2022 to May 2022, Ashby, without authority, knowingly removed documents and materials containing classified information. (Source)

Defense Logistics Agency Contractor Employees Involved In Scheme To Steal & Sell Government Property - March 6, 2025

Between October 2017 and September 2021, Christopher Hagan obtained stolen government items which he resold on online forums. One of Hagan's coconspirators, Jonathan Chaisson, 34, was employed by a national defense contractor based in New Hampshire and received used and / or broken Advance Target Pointer Illuminator Aiming Laser (ATPIAL) devices designated for military and law enforcement use. Chaisson stole or converted new and used parts and components to repair the ATPIALs and provided Hagan with the repaired devices to sell.

Hagan also conspired with Wade Walker, 45, and Michael Humphrey, 46, to steal and sell military equipment from the Defense Logistics Agency (DLA). Both Walker and Humphrey were employed by the DLA Red River Army Depot facility in Texarkana, Texas.

On multiple dates in 2019 and in 2020, Humphrey transferred stolen government property to Walker for resale, and Walker provided the stolen property to Hagan for further resale. Through the investigation, agents determined that Hagan had at least one customer in China.

Hagan was sentenced to prison. Chaisson pleaded guilty to conspiring to transport stolen property in interstate commerce and was sentenced to probation for two years.

Humphrey pleaded guilty to conspiring to sell stolen government property and was sentenced to probation for two years. Walker pleaded guilty to conspiring to sell stolen government property and was sentenced to probation for three years. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

2 DHS Employees Have Been Identified For Unauthorized Disclosure ICE Mass Deportation Plans - March 7,2024

Two people within the Department of Homeland Security have been accused of disclosing DHS operations amid the Trump administration's mass-deportation plans, Secretary Kristi Noem said.

"We have identified two leakers of information here at the Department of Homeland Security who have been telling individuals about our operations and putting law enforcement lives in jeopardy," she said. "We plan to prosecute these two individuals and hold them accountable for what they've done."

We are preparing to refer these perpetrators to the DOJ for felony prosecutions," she said. "These individuals face up to 10 years in federal prison. We will find and root out all leakers. They will face prison time, and we will get justice for the American people. (Source)

FBI Agent Charged With Disclosing Classified Information For Book He Was Writing - March 20, 2025

Johnathan Buma, a 15-year FBI veteran, was arrested as he was getting ready to board an international flight at John F. Kennedy International Airport in New York City.

Buma is accused of printing about 130 files of classified FBI documents and messages and later sharing the material with associates for a book he was writing about his career at the bureau.

The book draft contained information that Buma obtained through his position as an FBI Special Agent that relates to the FBI's efforts and investigations into a foreign country's weapons of mass destruction (WMD) program, according to the court document. On November 2, 2023, Buma wrote an email to various personal associates assisting him in negotiating a book deal with a publishing company. (Source)

Company Employee Pleads Guilty To Extortion Involving Massachusetts State Police & Commercial Driver's License Bribery Scheme - March 24, 2025

Eric Mathison pleaded guilty to his role in an extortion conspiracy involving former Massachusetts State Police (MSP) troopers who allegedly conspired to give false passing scores to certain Commercial Driver's License (CDL) applicants who had failed or had taken only partial CDL skills test, in exchange for bribes.

Mathison, who worked for a water company that employed drivers who needed CDLs to drive their delivery vehicles, admitted to his role in an alleged conspiracy with others including former MSP Sergeant Gary Cederquist, then in charge of MSP's CDL Unit, to give false passing scores to certain CDL applicants affiliated with the water company.

It is alleged that Cederquist gave passing scores to multiple applicants who actually failed the CDL skills test, as well as others who took only a partial test, in exchange for bribes of free inventory from the water company, such as cases of bottled Fiji, VOSS and Essentia water, cases of bottled Arizona Iced Tea and coffee and tea products, all of which Mathison delivered to an office trailer at the CDL test site in Stoughton.

Mathison admitted to his alleged communications with Cederquist about particular CDL applicants, their performance on the skills test, and inventory from the water company that Cederquist allegedly requested and that Mathison delivered. For example, Mathison admitted that he received texts, allegedly from Cederquist, describing one water company applicant as "an idiot," who had "no idea what he's doing," and "should have failed about 10 times already." It is alleged that Cederquist then gave this applicant a passing score. On another occasion, Mathison admitted that he asked Cederquist, "Hows the trailer holding," to which Cederquist allegedly responded, "In desperate need of restocking," along with a specific request for, among other things, premium bottled water, tea, energy drinks and a "truckload of large water." (Source)

Sheriff Sentenced To Prison For Accepting $75,000 In Bribes - March 21, 2025

Scott Jenkins is the former Sheriff of Culpeper County in Virginia. He was sentenced today to 10 years in federal prison for accepting over $75,000 in bribes in exchange for appointing numerous Northern Virginia businessmen as auxiliary deputy sheriffs within his department.

Jenkins accepted cash bribes and bribes in the form of campaign contributions from co-defendants Rick Rahim, Fredric Gumbinner, and James Metcalf, as well as at least five others, including two FBI undercover agents. Rahim, Gumbinner, and Metcalf have all pled guilty for their roles in the conspiracy.

In return for the bribes, Jenkins appointed each of the bribe payors as auxiliary deputy sheriffs, a sworn law-enforcement position, and issued them official Culpeper County Sheriff's Office badges and credentials. The bribe payors were not trained or vetted and did not render any legitimate services to the Sheriff's Office or the citizens of Culpeper County.

In addition, Jenkins pressured other local officials to approve a petition filed in Culpeper County Circuit Court by Rahim, a convicted felon, to restore his right to possess a firearm and which falsely stated that Rahim resided in Culpeper County. (Source)

Police Officer Pleads Guilty To $$35,000 COVID Emergency Loan Fraud - March 6, 2025

Kalynn Fields used two companies, founded in May and June 2022, to apply for an Economic Injury Disaster Loan and a Paycheck Protection Program Loan.

At the time, Fields was employed by the Metropolitan Police Department (MPD). Although Fields was required to report any outside business venture to MPD pursuant to MPD policies, Fields failed to do so. Neither company had a legitimate purpose, and each was created only to obtain EIDL and PPP loans. There were numerous false and fraudulent misrepresentations in the loan applications. As a result of the false information provided Fields received loans worth $35,000, which were later forgiven. (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

Former California Employment Development Department Employee Sentenced To Prison For Stealing $858,000+ & Taking Bribes - March 28, 2025

Regina Brice is a former employee of the California Employment Development Department (EDD). She was sentenced to prison for using her position to file $858,339 in fraudulent unemployment claims, effectively stealing money that was intended to give economic relief to people impacted by the pandemic.

Brice was employed by the EDD since 2010. During the pandemic, she was responsible for processing COVID-related unemployment claims.

However, between July 2020 and May 2021, Brice exploited her employee access at EDD to manipulate and file fraudulent unemployment claims for her co-conspirators in exchange for thousands of dollars in bribes. These co-conspirators included California prison inmates whom she instructed on how to bypass the system's fraud checking software to obtain the money. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

No Incidents To Report

CHURCHES / RELIGIOUS INSTITUTIONS

Bookkeeper Accused For Embezzling At Least $400,000 From Church Over 7 Years / Used Funds To Pay Credit Cards, Travel, Etc. - March 14, 2025

Corie Boyer was responsible for maintaining the parish's books and records, organizing certain parish fundraisers and assisting in the collection and counting of the weekly offertory.

From at least January of 2017 through March of 2024, Boyer stole at least $400,000 in parish funds in multiple ways. She used parish funds to pay her personal credit card bills and used parish credit cards for personal expenses including airfare for herself and relatives, cruises, college tuition payments, shopping, taxes and rent, the indictment says. She also wrote checks to herself and stole cash from the offertory, and she covered up her thefts by falsifying parish records, the indictment says. (Source)

Office Manager For Synagogue Admits To Embezzling $350,000 Over 4 Years - March 20, 2025

In 2010, Stacy Margaritondo began working at the synagogue located in Union County, New Jersey and was promoted to office manager and bookkeeper in July 2020.

From December 2019 through May 2023, Margaritondo abused this position of trust by engaging in a fraudulent scheme to misappropriate approximately $350,000 from the synagogue's accounts. As part of the scheme, Margaritondo routinely issued unauthorized checks made payable to herself drawn on the synagogue's bank accounts; obtained unauthorized additional funds to conceal the embezzlement scheme by fraudulently using the synagogue's name, bank statements, and balance sheet to obtain short-term financing from at least three cash advance companies; and intentionally kept inaccurate accounting records and altered bank statements that she provided to the board of directors to conceal her scheme. (Source)

Church Pastor & Ex-Political Candidate Arrested For $230,000+ Wire Fraud Schemes Targeting Friends, Nonprofit Corporation - March 7, 2025

A pastor at a San Bernardino church and one-time political candidate for the San Bernardino City Council has been arrested on an 11-count federal grand jury indictment alleging he committed several con jobs targeting long-time friends and a nonprofit corporation tied to another church, swindling them out of a total of more than $230,00. (Source)

LABOR UNIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

Morgan Stanley Financial Advisor Sentenced To Prison For $5 Million+ Fraud Scheme - March 27, 2025

Jesus Rodriguez de la Cruz, 46, defrauded his financial services employer, Morgan Stanley, and clients of money through materially false pretenses, representations and promises. Rodriguez de la Cruz orchestrated fraudulent transfers of funds from the bank accounts of Morgan Stanley and clients to other bank accounts for his own benefit.

In all, Morgan Stanley suffered a total loss of $5,554,968.10 due to Rodriguez de la Cruz's scheme. (Source)

Credit Union Employee Sentenced To Prison For Stealing $772,000+ - March 4, 2025

Kevin Spratt worked as a senior branch sales representative at a federally insured credit union (FCU) located in South Philadelphia. His duties included opening accounts, processing loan applications, and any branch duty other than depositing and withdrawing customer monies.

Spratt was sentenced to prison and five years of supervised release for defrauding a credit union and multiple credit union members of approximately $772,155.84 through a combination of fraudulent loans and unauthorized withdrawals. Spratt was also ordered to pay $822,155.84 in restitution.

From October 1, 2018, and continuing through on or about September 15, 2022, Spratt stole money from the FCU by, unbeknownst to 10 credit union members, taking out a total of approximately 32 loans in their names and converting the loan proceeds to his own use.

From February 14, 2020, through on or about September 28, 2022, he stole money from 12 FCU members by routinely withdrawing funds from their accounts without the members' authorization. Six of these FCU members' names had been used in the aforementioned fraudulent loan scheme.

Spratt deceived credit union tellers into facilitating the withdrawal of money from member accounts by, among other things, providing photocopies of the members' driver's licenses to the tellers as evidence that the absent members were in the credit union at the time of each withdrawal.

The teller would enter the information provided by Spratt into a computer, which would allow Spratt to retrieve the member funds he sought from a cash machine. After receiving that money, he converted the funds to his own use. (Source)

Bank Employee Pleas Guilty To Embezzling $190,000+ Of Deceased Customer's Money - March 19, 2025
Billy Gedeon, 34, used his position as an employee at an international financial institution to embezzle over $190,000 from a deceased customer's accounts.

Gedeon admitted the following: After learning that one of the bank's regular customers had died, Gedeon went into the deceased customer's accounts several times without authorization. In 2023, Gedeon stole over $190,000 from one of the accounts by forging the deceased customer's signature on a bank form (which closed the account), withdrawing all the money, and depositing it into Gedeon's personal account at another bank. (Source)

Bank Teller Pleads Guilty To Stealing $180,000+ From Customer Accounts - March 4, 2025
While working as a teller at a bank branch in Boston, Derek Aut stole from the bank accounts of two customers by forging the victims' names on withdrawal slips. When one of the victims noticed money missing from her account, Aut allegedly attempted to cover his theft by taking money from the other victim's account and depositing it into the first victim's account.

In total, Aut is alleged to have taken more than $180,000 from the victims' accounts. (Source)

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

Supervisor For Recovery Connections Centers Of America Sentenced To Prison For Defrauding Medicare & Medicaid Out Of $3.5 Million+ - March 5, 2025
In pleading guilty in November 2023 to a charge of conspiracy to commit health care fraud, Mi Ok Song Bruining, 64, admitted that, while employed as a supervisor at Recovery Connections Centers of America, Inc. (RCCA) in Providence, Rhode Island, she helped devise and execute a scheme that shortchanged Rhode Island and Massachusetts substance abuse disorder patients out of counseling and treatment services while, at the same time, defrauding Medicare, Medicaid, and other health insurers out of more than $3.5 million dollars.

Bruining, and others working at her direction, routinely submitted false and fraudulent claims for psychotherapy and counseling services that did not occur for the length of time billed, consistently billing for far more patients than was possible for RCCA staff to have seen during office hours. Bruining, known at RCCA as the "Five Minute Queen" for her speed in seeing patients for so-called counseling sessions, billed for 45-minute sessions when she actually saw patients for no more than 5-10 minutes, at times asking patients only one question before she ended a session. (Source)

Office Manager For Medical Group Practice Sentenced To Prison For Stealing $140,000+ Over 3 Years - March 7, 2025
Elizabeth Morse was a long-time employee of Bedford Women's Care Associates (BWCA), a Bedford, New Hampshire medical group practice that specialized in Obstetrics & Gynecology until its closure in early 2023.

Starting in 2020, Morse became BWCA's office manager and handled the processing of payroll through a third-party servicer. Morse manipulated the payroll processes at BWCA by logging into the third-party servicer and changing her rate of pay to a higher amount than what she was entitled. The defendant's scheme lasted approximately three years. Morse was also ordered to pay restitution in the amount of $168,311.40. (Source)

Hospital Pharmacy Technician Sentenced To Prison For Stealing Drugs And Distributing - March 11, 2025

Between Dec. 30, 2022 and April 9, 2023, Curtis Green used his position as a certified pharmacy technician for a hospital in Mayfield Heights, Ohio, to order controlled substances during the course of his employment.

Green ordered on behalf of the hospital, but he used the drugs his own unlawful distribution. During this time, Green was found to possess 103 grams of oxycodone and 77.5 grams of a mixture and substance containing a detectable amount of fentanyl, all schedule II controlled substances.During a federal search warrant execution of Green's residence on April 9, 2023, agents seized $72,880 in cash. An additional $2,025 was seized from the defendant on the following day. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

No Incidents To Report

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

Employee Pleads Guilty To Stealing Trade Secrets From Employers To Build Business With China Company - February 27, 2025

Liming Li pleaded guilty today to illegally possessing sensitive technologies that he downloaded from his Southern California-based employers and used them to market his own competing company to a China-based company.

From 1996 to 2013, Li worked for a Southern California-based business identified in court documents as "U.S. Company #1," which specialized in precision measuring instruments and metrological technology and equipment. The company designed and sold a range of products such as micrometers, calipers, coordinate measuring machines (CMMs), and optical measurement systems.

Li worked at U.S. Company #1 as a senior software engineer, then as a program manager. From 2013 to 2018, Li worked as chief technologist at a wholly-owned subsidiary of U.S. Company #1. During his employment at U.S. Company #1 and its subsidiary, Li worked on the development of the source code for one of the company's software programs, which was considered its proprietary information.

In July 2013, Li signed an employee handbook and confidentiality agreement with U.S. Company #1 that required him to turn over all writings, records, files, technology, trade secrets or data containing any proprietary information belonging to the company. The agreement also prohibited Li from copying the company's proprietary information without written permission.

Li admitted in his plea agreement that he occasionally downloaded the company's proprietary information onto his personal devices without permission. Li failed to return all the proprietary information belonging to U.S. Company #1 after its subsidiary terminated him in January 2018.

In February 2018, Li operated a consulting company named JSL Innovations Inc. and in March 2020, he signed an employment agreement with Suzhou Universal Group Technology Co. Ltd., a China-based chain-and-bearing manufacturer. Li continued to work for Suzhou Universal until his arrest in May 2023.

During this period, Li continued to knowingly possess U.S. Company #1's proprietary information and – more than once – accessed this information without that company's authorization.

Li admitted that he used the proprietary information for his own economic benefit and that it would injure U.S. Company #1's interests. (Source)

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

Homeowners Association (HOA) Property Manager Admits To Embezzling $2.1 Million From HOA's - March 27, 2025

Blake Cozzens, a property manager pleaded guilty today to wire fraud and bank fraud after admitting he embezzled funds from homeowners associations, property owners, and tenants in Cedar City, He also admitted to fraudulently presenting cashier's checks to Las Vegas casinos.

From January 2020 to January 2025, Cozzens was the property manager for multiple HOAs and property owners in Iron County, Utah. Cozzens admitted to defrauding HOAs, property owners, and tenants by embezzling funds he was responsible for safekeeping and diverting the funds for his own use. He also submitted fraudulent deposits to an online application that helps manage properties.

The California corporation that offers the application lost $210,000 due to Cozzens' fraudulent conduct. As a result of the scheme, Cozzens fraudulently obtained at least $772,966 from HOAs, property managers, tenants, and the California corporation.

In addition, Cozzens admitted to defrauding a bank in Las Vegas. He did so by presenting seven cashier's checks totaling $1,414,000 to Las Vegas casinos in exchange for markers, i.e., credits to gamble. After gambling, Cozzens then falsely reported to the bank that he had lost the checks, causing the bank to stop payments to the casinos. Cozzens caused the bank to lose $1,395,673.58. (Source)

Operations Manager For Property Management Company Sentenced To Prison For Stealing $2 Million+ - March 17, 2025

Marcie Doty was employed as an Operations Manager for a property management business located in Evansville, Indiana.

Between May 2017 and June 2022, Doty ran a five-year wire fraud scheme, stealing approximately $1,803,466.38 from her employer via unauthorized checks and Automated Clearing House (ACH) transfers.

During this five-year period, Doty executed 99 unauthorized ACH transfers, totaling $503,151.59 and wrote 279 unauthorized checks to herself, totaling $1,300,314.79. The funds were transferred from her employer's bank accounts to her personal bank accounts. In an effort to conceal the unauthorized checks, Doty entered false information in the business accounting software, representing that the checks were written to her employer instead of herself. These false entries made it appear as if the business's funds were being moved from one account to another for a legitimate business purpose.

In January 2017, Doty agreed to purchase a 25% equity share in her employer's business. Doty used some of the money she stole via the wire fraud scheme to make payments towards her purchase of the 25% equity share.

Doty has also been ordered to pay $2,517,343.05 in restitution. (Source)

Business Financial Manager Sentenced To Prison For Embezzling $1.7 Million+ - March 27, 2025
From 2016 to 2023, Kristin Turney executed a scheme to defraud her employer, a small, family-owned business, by embezzling more than $1.7 million.

Turney was in charge of the company's financial matters, including bank accounts, payroll, accounts payables and receivables, and tax filings. During the scheme, Turney misused her access and control over the company's bank accounts and books and records to write herself company checks, which she then deposited into bank accounts she controlled. Turney made over 1,000 unauthorized bank deposits to herself totaling over $1.7 million. Court documents show that Turney covered up the fraud by making false accounting entries in the company's books and records. She also provided fraudulent information to the company's tax return preparer and lied to the company's owner and employees. As a result of Turney's embezzlement scheme, the company continues to be impacted by the defendant's theft. (Source)

Employee Admits To Embezzling $1.7 Million+ From His Employer Over 3 Years By Redirecting Funds To Personal Bank Account - - March 17, 2025
Beginning in 2021 and continuing until October 2024, Timothy Edgar defrauded his employer to obtain money and property by stealing and lying.

As part of Edgar's scheme, he fraudulently opened a sales channel through a popular online marketplace and used his employment credentials to access the vendor portal and redirect Automated Clearing House payments to his personal bank account. Edgar then made payments back to his employer using his personal credit card. Edgar embezzled approximately $1,778,251 from his employer. (Source)

Vice President of Pharmaceutical Company Admits To Insider Trading To Avoid $1.3 Million Loss - March 7, 2025
George Demos, then-vice president at San Diego-based Acadia Pharmaceuticals Inc., pleaded guilty in federal court to illegally selling 60,000 company shares, thus avoiding a $1.3 million loss by acting on insider knowledge about the labeling process for a prescription drug with the Food and Drug Administration (FDA).

Demos, a medical doctor who was the Vice President of Drug Safety and Pharmacovigilance and member of the drug label team at publicly-traded Acadia, admitted that he was able to avoid the loss by dumping his shares just two hours before negative news about the labeling process became public.

Through his positions, Demos had access to material information belonging to Acadia, including the drug approval and labeling process with the FDA, before the information was released to the investing public. As an employee of Acadia, Demos was subject to an insider trading policy that prohibited trading in company stock on the basis of material nonpublic information. (Source)

Company Financial Controller Charged With Embezzling $1 Million / Falsified Employment Documents To Conceal His Lack Of Legal Status - March 20, 2024
Between January 2016 and June 2023, Sergio Lopez abused his position as the accounting supervisor and controller to defraud a family-run Fresno fruit wholesaler in California.

Lopez would write multiple company checks payable to "cash" and then deposit them into his own personal bank account through local ATMs. He signed the fraudulent checks using the signatures of other employees with signatory authority, including one of the founders of the company.

Through this scheme, Zacarias Lopez embezzled more than $1 million before he was eventually detected by one of the banks and terminated by the company. To secure his accounting role in the first place, Lopez stole a valid social security number and used that along with other falsified employment documents to conceal his lack of legal status. The indictment also states that Lopez was previously removed from the United States in 2000 and has not been permitted to return to the United States. (Source)

Company Bookkeeper Sentenced To Prison For Stealing $439,000+ - March 26, 2025

Mary Katicih used her position as bookkeeper for a Belle Chasse, Louisiana-based company, to fraudulently divert funds for her own benefit, from the company's bank accounts.

Katicih also purchased personal items using company funds.

Katicih was ordered to pay restitution in the amount of $439,650.51 to the owner of the company. (Source)

Payroll Manager Pleads Guilty To Embezzling $400,000+ From Her Employer - March 12, 2025

Courtney Gregory, 47, was employed by a security services company in Norfolk. Her position gave her access to the company's bank accounts and permitted her to alter the payment information for employees in the company's systems.

In February 2023, a review of the payroll system revealed multiple gaps in the sequence of company checks. Through a review of banking records, the company discovered hundreds of additional checks that had not been recorded in the payroll system and that had been paid to inactive former employees of the company.

Further review of the system logs associated with the company's payroll system reflected that the routing number and account numbers where funds were sent via direct deposit had also been changed for various former employees. Those logs showed that, using the login information assigned to her, Gregory had accessed the system, reactivated employee profiles, and, after payments were made to those former employees, deleted the records of the payments.

From February 2022 through February 2023, Gregory made over one hundred transfers from the company's accounts to her own personal bank account, as well as hundreds of other unauthorized automated clearing house (AHC) transfers. In total, $136,145.68 was taken from the company using physical checks and another $283,064.62 was taken from the company's accounts using unauthorized electronic transfers.

Gregory embezzled $419,210 from her employer. (Source)

Employee Sentenced To Prison For Embezzling $250,000+ From Over 5 Years - March 12, 2025

Christy Myers, 64, through a variety of methods, embezzled approximately $250,400 from her employer between April 2016 and June 2021.

Myers had been previously convicted and sentenced to a term in federal prison in connection with a mortgage fraud scheme in 2007. (Source)

Automobile Dealership Office Manager Sentenced To Prison For Embezzling $192,000+ - March 19, 2025
Between 2001 and January 2024, Jennifer LaBonte was employed by automobile dealerships located in Burlington. From about 2012 until her termination, LaBonte served as office manager for the dealerships, a position that gave her oversight over all accounting matters. LaBonte had check-signing authority.

LaBonte began embezzling from the dealerships. For the most part, LaBonte stole cash receipts that had been paid over by dealership customers, but she also issued checks to herself for non-business-related purposes. LaBonte tried to cover up her thefts by manipulating and falsifying entries about individual transactions in the dealerships' computerized accounting systems. An officer at the dealerships uncovered the fraud in January 2024 and LaBonte was immediately fired. LaBonte was ordered to pay $192,675 in restitution. (Source)

Office Manager Sentenced To Prison For Embezzling $158,000+ - March 5, 2025
Angela Cooper embezzled more than $158,000 and stole the identity of a coworker while employed by AMK Heating and Cooling in Edwardsville, Illinois,

Cooper served as the office manager for AMK and had access to the company's checkbook and accounting software. Using these tools, Cooper fraudulently wrote more than 100 checks payable to herself and forged the signature of the business's owner.

Cooper tried to conceal her fraud by disguising the checks as payroll and loans to her from AMK. Over a two-year period, Cooper embezzled $158,658.41 from AMK.

While employed by AMK, Cooper also had access to employee files and personal information like birthdates and social security numbers. Cooper used a coworker's information to apply for and fraudulently obtain a Discover credit card. Cooper maxed out the credit card, accruing $9,877.71 in charges on the card in a matter of weeks. (Source)

EMPLOYEES' WHO EMBEZZLE / STEAL MONEY FOR PERSONAL ENRICHMENT AND TO LIVE ENHANCED LIFESTYLE OR TO SUPPORT GAMBLING OR DEBT PROBLEMS
Employee Of Online Car Sales Company Sentenced To Prison For Embezzling $2 Million For 3 Years / Used Funds For Lavish Lifestyle & Luxury Automobiles - March 12, 2025
Beginning in October 2018 John Whisenant worked in a variety of roles at the online used car sales company. About a year after he began with the company, Whisenant was promoted into a role where he had access to the company bank accounts and accounting software.

Beginning in about June 2019 and continuing until November 2021, Whisenant used his access to make 57 wire transfers totaling over $2 million into accounts he controlled. Whisenant disguised the transfers as legitimate business expenses in the company's accounting software with a variety of false entries. Whisenant defrauded the company of $2,084,799.

Whisenant used some of the money for a lavish lifestyle. He bought luxury automobiles such as Porches and Mercedes. He spent $123,096 for a 2022 Audi E-Tron and bought a $98,100 Tesla. He rented luxury homes in Southern California and purchased two airline tickets to Paris at a cost of nearly $23,000 each. More than $1 million went to pay his credit card debts.

The fraud on the company accounts was discovered when a bookkeeper began a more comprehensive review of the company's financials in January 2022. Whisenant resigned abruptly in February 2022.

When confronted by the FBI, Whisenant tried to blame the embezzlement on the company CEO. As prosecutors noted in their sentencing memo the impact on the company has been severe. "Whisenant's fraud seriously harmed his victims. His betrayal "traumatized" his co-workers and destabilized the company's finances.

Just before his July 2024 sentencing date, Whisenant sent an email to his pretrial services officer saying, "I'm not ready to go to jail yet." Despite his efforts to evade police, the FBI located and arrested him on August 14, 2024. (Source)

Office Manager Of Senior Assisted Living Facility Sentenced To Prison Embezzling $1.5 Million / Used Funds To Buy Pickup Truck & Gamble - March 20, 2025

Amy Curry worked as an office manager and bookkeeper at Silver Bluff, LLC (Silver Bluff), a senior living and care facility in Canton, North Carolina.

As part of her duties, Curry had access to and control over Silver Bluff's bank accounts and accounting records. From December 2022 to April 2023, Curry made at least 154 unauthorized bank transfers totaling over $1.5 million from the facility's bank accounts to bank accounts controlled by Curry and her then-boyfriend, J.C. To avoid detection, Curry deleted the wire transfer history from Senior Bluff's bank accounts and altered the notification settings to prevent Silver Bluff employees and management from receiving alerts.

Curry also made handwritten notes on Senior Bluff's bank statements, falsely noting that the fraudulent transfers were for payroll.

Court records show that Curry used the embezzled funds to pay for personal expenses, including to purchase a pick-up truck. Curry and J.C. also spent over $700,000 of the embezzled funds gambling at casinos. Curry embezzled at least $1.5 million. (Source)

Company Financial Controller Sentenced To Prison For Embezzling $665,000+ Over 6 Years To Supporting Gambling Problems - March 26, 2025

Jesse Sherman began working for Sims Vibration Laboratory Inc. in 2008. In his role as controller, he had complete access and control of the company accounting systems and banking functions.

Between 2012 and 2018, Sherman began abusing the trust the company had placed in him, by using a variety of schemes to steal from the company. Sherman made false representations to the company's owner and President, he created false business records, and he created payroll checks and other checks that he deposited in his own accounts. In some instances, he noted in the company books that the check was "void" even though he had cashed it.

Sherman's fraud resulted in a loss to the company of at least $665,840. As a Certified Public Accountant Sherman knew that he owed taxes on the money he obtained by fraud, but he failed to pay the $202,196 he owed on his taxes between 2013 and 2018.

Sherman claims his gambling drove his behaviors. (Source)

Tech Employee Sentenced To Prison For Embezzling $550,000+ / Used Funds For Trips, Private Jets, Luxury Hotels, Etc. - March 21, 2025

The first scheme began in 2019, when Westcott Curley embezzled money from his then-employer by misusing cloud computing resources and accounts available to him as an employee. Curley used employer funds and his employee work authorizations to purchase cloud computing resources, then sell or lease them back to the company, paying himself with company money at many times their market value. Through this scheme he obtained more than $550,000, and he was caught while attempting to obtain another half-million dollars. He spent significant portions of the proceeds on extravagances, such as trips on private jets, luxury hotel stays and a penthouse apartment at Seattle's Harbor Steps complex. Even after Francis-Curley was caught and fired, he emailed customer service and corporate executives in an effort to receive an additional half-million dollars.

In 2020, Curley defrauded the Paycheck Protection Program (PPP), a COVID assistance program designed to help small businesses and their employees weather the pandemic. Francis-Curley filed paperwork claiming that two companies he controlled qualified for assistance, when in fact they had no payroll and did not qualify for relief. He obtained nearly $100,000 and spent much of it on personal goods and services.

Finally, in October 2022, Curley applied for and obtained a credit card in the name of his former significant other. Curley used the card for more than $1,000 in personal expenditures. (Source)

Employee Sentenced To Prison For Embezzling $440,000 From 2 Different Employers / Used Funds To Pay Credit Cards - March 11, 2025

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

Between May 2022 and December 2023, Botelho improperly inflated her payroll from another employer by more than $160,000. She concealed her scheme by manipulating her employer's payroll and accounting software to hide her inflated payroll as well as phony "reimbursements" she paid herself.

Botelho was also ordered to pay restitution and forfeiture orders of $443,122.59. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Company Employee Charged With Stealing $28 Million By Creating Fake Company And Diverting Funds - March 26, 2025

Between 2011 and 2023, Paul Steed was employed by Mars Wrigley, a subsidiary of Mars. Inc. (Mars), working remotely from his home in Stamford, Connecticut. Steed served as Global Price Risk Manager for Mars Wrigley's Global Cocoa Enterprise. As part of his employment, Steed was responsible for managing Mars Wrigley's participation in the U.S. Department of Agriculture (USDA) Sugar-Containing Products Re-Export Program.

In approximately 2016, Steed created a company, MCNA LLC, to mimic an actual Mars entity, Mars Chocolate North America. He then diverted millions of dollars in Mars assets to a bank account he set up in MCNA's name by directing sugar refineries purchasing Mars's re-export credits, obtained through the USDA program, to pay MCNA LLC as if it were a legitimate Mars entity.

Steed is alleged to have stolen more than $28 million from Mars and through his schemes.

More than $18 million was seized today for forfeiture, and the government is seeking to forfeit a Greenwich home that Steed is alleged to have purchased with nearly $2.3 million in stolen funds. It is alleged that another $2 million was sent by Steed to Argentina, where he is a dual citizen, has family ties, and owns a ranch. (Source)

Boyfriend Of A Senior Level Employee For Pharmaceutical Company Sentenced To Prison For $2.3 Million Fake Invoice Scheme / Used Funds To Purchase Mercedes-Benz, Diamond Engagement Ring, Freightliner Trucks And A $1.9 Million Condo - March 10, 2025

The boyfriend of a senior level employee at the multinational pharmaceutical company Takeda Pharmaceutical Company Limited (Takeda) was sentenced to prison for setting up a fake consulting company that billed Takeda for services it never actually provided.

Montronde was also ordered to pay $2.3 million in restitution. Montronde was arrested and charged in January 2023 along with his girlfriend Priya Bhambi a former senior employee in the technology operations group of Takeda.

In 2022, Montronde and Bhambi orchestrated and executed a scheme to defraud Takeda of at least $2.3 million in payments for purported consulting services by submitting fabricated invoices on behalf of a sham consulting company.

Bhambi had previously engaged in the same fraud using a different sham consulting company, resulting in payments from Takeda totaling nearly $300,000 for consulting services that were never provided.

In February 2022, Montronde and Bhambi incorporated a sham consulting company, Evoluzione Consulting LLC (Evoluzione). Later, Bhambi created a website for Evoluzione with false information, including fabricated blog posts, to make it appear that Evoluzione was a legitimate consulting business.

After incorporating Evoluzione, Bhambi, in coordination with Montronde, submitted a statement of work to Takeda and caused Takeda to sign a master services agreement with Evoluzione and issue a purchase order to Evoluzione for consulting services with a total cost of $3.542 million. Then, between March and May of 2022, Bhambi and Montronde fabricated and submitted five separate invoices to Takeda for services that Evoluzione had not performed, each in the amount of $460,000. The defendants also created a fictional employee "Jasmine" to handle communications with Takeda.

When questioned by Takeda employees, Bhambi made false representations regarding the services purportedly provided by Evoluzione. Before discovering the scheme and terminating Bhambi, Takeda, relying on these false representations, paid all five of the invoices to business accounts opened by Montronde in the name of Evoluzione.

The couple used the fraudulently obtained funds to purchase a Mercedes-Benz Model Class E, a diamond engagement ring, freightliner trucks, a $1.9-million 2-bedroom condo in Boston's Seaport District and a $50,000 wedding venue deposit. These assets are now subject to the Court's forfeiture order. (Source)

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

Software Developer Convicted For Adding Killing Switch To MS Windows Active Directory That Sabotaged IT Systems After He Was Fired - March 7, 2025

Davis Lu, 55, was employed as a software developer for his employer headquartered in Beachwood, Ohio, from November 2007 to October 2019.

Following a 2018 corporate realignment that reduced his responsibilities and system access, Lu began sabotaging his employer's systems. By Aug. 4, 2019, he introduced malicious code that caused system crashes and prevented user logins.

Specifically, he created "infinite loops" (in this case, code designed to exhaust Java threads by repeatedly creating new threads without proper termination and resulting in server crashes or hangs), deleted coworker profile files, and implemented a "kill switch" that would lock out all users if his credentials in the company's active directory were disabled. The "kill switch" code — which Lu named "IsDLEnabledinAD", abbreviating "Is Davis Lu enabled in Active Directory" — was automatically activated upon his termination on Sept. 9, 2019, and impacted thousands of company users globally. Lu named other code "Hakai," a Japanese word meaning "destruction," and "HunShui," a Chinese word meaning "sleep" or "lethargy." Additionally, on the day he was directed to turn in his company laptop, Lu deleted encrypted data. His internet search history revealed he had researched methods to escalate privileges, hide processes, and rapidly delete files, indicating an intent to obstruct efforts of his co-workers to resolve the system disruptions. Lu's employer suffered hundreds of thousands of dollars in losses as a result of Lu's actions. (Source)

THEFT OF ORGANIZATIONS ASSESTS

Augusta National Golf Club Employee Sentenced To Prison For Stealing Gold Tournament Memorabilia For 13 Years & Selling To Online Broker For $5.3 Million - March 20, 2024

Richard Globensky admitted in a plea agreement that he stole the merchandise and memorabilia from 2009 to 2022 while he was employed by the club as a warehouse assistant. The merchandise included Masters shirts, hats, flags, watches, and other goods, while the memorabilia included historically significant items, such as the Green Jackets awarded to tournament winners Arnold Palmer, Gene Sarazen, and Ben Hogan. Globensky sold the merchandise to an online broker in Florida for a total of approximately $5.3 million. He sold the historically significant memorabilia to the same broker, as well as to the broker's associate, for nearly $300,000. The brokers later re-sold the stolen merchandise and memorabilia, often at significant markups from the amounts paid to Globensky. At least one of the stolen items was purchased by a collector in Chicago.

During the last six years of the crime, Globensky spent more than $370,000 to purchase five vehicles and a motorboat, as well as more than $160,000 for Walt Disney-themed vacations and related activities. Globensky also spent nearly $600,000 on construction of a custom-built residence in Georgia and approximately $32,000 at luxury retailer Louis Vuitton. (Source)

Employee Working For Multinational DVD Company Charged With Stealing, Selling Pre-Release Commercial DVDs For Blockbuster Films - March 6, 2025

Steven Hale, 37, worked for a multinational company that, among other things, manufactured and distributed DVDs and Blu-rays of movies.

From approximately February 2021 to March 2022, Hale allegedly stole numerous "pre-release" DVDs and Blu-rays, that is, discs being prepared for commercial distribution in the United States, and not available for sale to the public.

These included DVDs and Blu-rays for such popular films as "F9: The Fast Saga," "Venom: Let There Be Carnage," "Godzilla v. Kong," "Shang-Chi and the Legend of the Ten Rings," "Dune," and "Black Widow." Hale allegedly sold the DVDs and Blu-rays through e-commerce sites.

At least one pre-release Blu-ray that Hale allegedly stole and sold, "Spider-Man: No Way Home," was "ripped" — that is, extracted from the Blu-ray by bypassing the encryption that prevents unauthorized copying — and copied. That digital copy was then illegally made available over the internet more than a month before the Blu-ray's official scheduled release date. Copies of "Spider-Man: No Way Home" were downloaded tens of millions of times, with an estimated loss to the copyright owner of tens of millions of dollars. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG & ALCOHOL RELATED INCIDENTS

Nurse Working At Healthcare Facilities Sentenced To Prison For Stealing Morphine - March 25, 2025

Between January 2023 and August 2023, Abigail Hall worked as a contract registered nurse at several facilities in Kentucky, including a health care facility in Lawrenceburg, Ky., that focused on care for the elderly and infirm.

Hall admitted that on August 27, 2023, she took morphine that had been prescribed for three patients that she was treating at the healthcare facility, all of whom had significant disease and pain concerns.

Hall replaced the stolen morphine with water and blue food coloring, to resemble the real medication. Ultimately, Hall took at least seven syringes of stolen morphine and administered the tampered morphine to at least one of the patients. (Source)

OTHER FORMS OF INSIDER THREATS

North Carolina Department Of Transportation Employee Pleads Guilty To The Sale Of 2,500 Dangerous Counterfeit Car Airbags - March 11, 2025

Mateen Alinaghian pled guilty today to importing thousands of counterfeit car steering wheel airbags into the Raleigh, NC area over the past two years. The counterfeit airbags were sold locally and to online buyers through Facebook Marketplace.

Alinaghian imported approximately 2,500 counterfeit air bags into Raleigh between May 2022 and April 2024. Alinaghian imported steering wheel airbags with counterfeit markings of Honda, Chevrolet, General Motor, and Toyota, from a supplier in the United Kingdom.

Alinaghian then sold the counterfeit airbags to unsuspecting customers using Facebook Marketplace. Alinaghian used the Facebook Marketplace seller profile of "Matt AutoParts" or "Medo Smith" to advertise and sell the counterfeit airbags. Alinaghian is currently employed as an engineer with the N.C. Department of Transportation.

According to testing done by Honda, General Motors, and Toyota, the steering wheel airbags obtained and sold by Alinaghian were not manufactured by the car companies, and often included materials of lesser quality. In testing, the counterfeit airbags often malfunctioned, either not fully inflating or inflating late – posing a potentially serious risk of injury to the vehicle driver.

After identifying that Alinaghian was importing the counterfeit airbags from a source in the United Kingdom, HSI contacted law enforcement abroad. As a result, a search warrant was executed on September 19, 2024, by the City of London Police's Intellectual Property Crime Unit (PICU). PICU officers searched two residential and one business address and seized a total of 500 counterfeit airbags and an estimated £140,000 in cash. Three men were arrested on suspicion of fraud by false representation, conspiracy to commit money laundering, and conspiracy to distribute counterfeit goods. The investigation is still ongoing. (Source)

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS
No Incidents To Report

EMPLOYEES' NON-MALICIOUS ACTIONS CAUSING DAMAGE TO ORGANIZATION
No Incidents To Report

EMPLOYEES' MALICIOUS ACTIONS CAUSING EMPLOYEE LAYOFFS OR CAUSING COMPANY TO CEASE OPERATIONS
No Incidents To Report

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'
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.

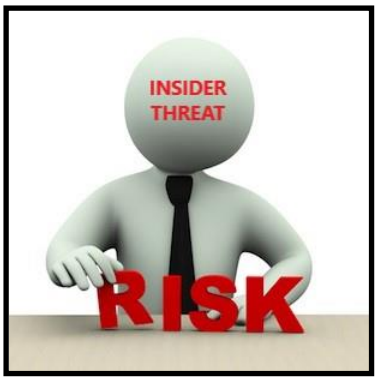
TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

- ☐ 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

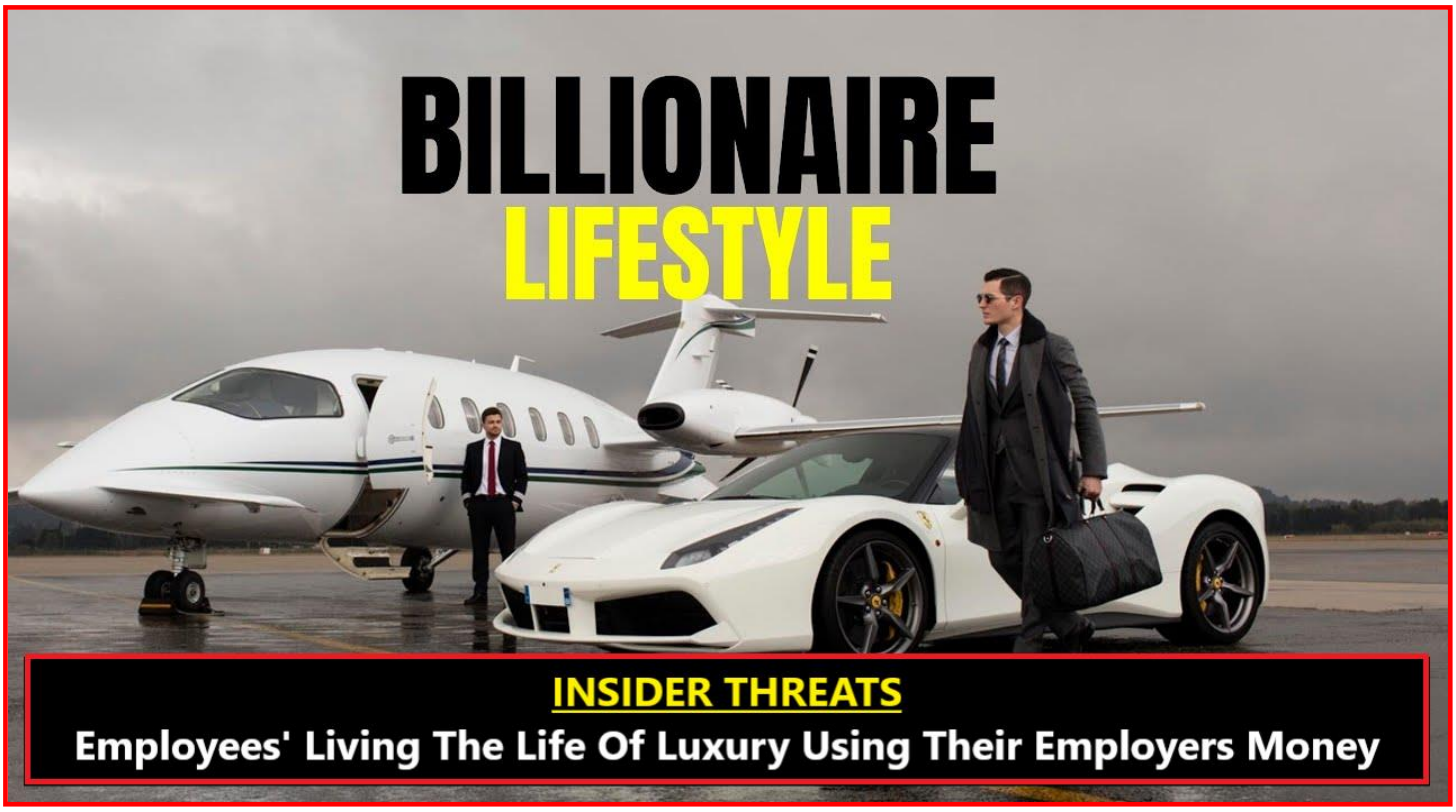
- ☐ Bribery, Extortion, Blackmail

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 WERE THE 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

2 Former Employees Of Mortgage Lending Business Charged For Roles In $3 BILLION Mortgage Fraud Scheme - November 13, 2024

Christopher Gallo and Mehmet Ali Elmas were previously employed by a New Jersey-based, privately owned licensed residential mortgage lending business.

Gallo was 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 approximately $3 billion in loans. (Source)

TD Bank Pleads Guilty To Money Laundering Conspiracy By Bribed Employees / FINED $1.8 BILLION - October 10, 2024

TD Bank failures made it "convenient" for criminals, in the words of its employees. These failures enabled three money laundering networks to collectively transfer more than $670 million through TD Bank accounts between 2019 and 2023.

Between January 2018 and February 2021, one money laundering network processed more than $470 million through the bank through large cash deposits into nominee accounts. The operators of this scheme provided employees gift cards worth more than $57,000 to ensure employees would continue to process their transactions. And even though the operators of this scheme were clearly depositing cash well over $10,000 in suspicious transactions, TD Bank employees did not identify the conductor of the transaction in required reports.

In a second scheme between March 2021 and March 2023, a high-risk jewelry business moved nearly $120 million through shell accounts before TD Bank reported the activity.

In a third scheme, money laundering networks deposited funds in the United States and quickly withdrew those funds using ATMs in Colombia. Five TD Bank employees conspired with this network and issued dozens of ATM cards for the money launderers, ultimately conspiring in the laundering of approximately $39 million. The Justice Department has charged over two dozen individuals across these schemes, including two bank insiders. (Source)

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)

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)

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)

CEO Of Bank Sentenced To Prison For $47 Million Fraud Scheme That Caused Bank To Collapse - August 19, 2024

While the CEO of Heartland Tri-State Bank (HTSB) in Elkhart, Shan Kansas, Hanes initiated 11 outgoing wire transfers between May 2023 and July 2023 totaling $47.1 million of Heartland's funds to a cryptocurrency wallet in a cryptocurrency scheme referred to as "pig butchering."

The funds were transferred to multiple cryptocurrency accounts controlled by unidentified third parties during the time HTSB was insured by the Federal Deposit Insurance Corporation (FDIC). The FDIC absorbed the $47.1 million loss. Hanes' fraudulent actions caused HTSB to fail and the bank investors to lose $9 million. (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
Anesthesiologist Working At Surgical Center Sentenced To 190 Years In Prison For Tampering With IV Bags / Resulting In Cardiac Emergencies & Death - November 20, 2024
Raynaldo Ortiz, a Dallas, Texas anesthesiologist was convicted for injecting dangerous drugs into patient IV bags, leading to one death and numerous cardiac emergencies.

Between May and August 2022, numerous patients at Surgicare North Dallas suffered cardiac emergencies during routine medical procedures performed by various doctors. About one month after the unexplained emergencies began, an anesthesiologist who had worked at the facility earlier that day died while treating herself for dehydration using an IV bag. In August 2022, doctors at the surgical care center began to suspect tainted IV bags had caused the repeated crises after an 18-year-old patient had to be rushed to the intensive care unit in critical condition during a routine sinus surgery.

A local lab analyzed fluid from the bag used during the teenager's surgery and found bupivacaine (a nerve-blocking agent), epinephrine (a stimulant) and lidocaine (an anesthetic) — a drug cocktail that could have caused the boy's symptoms, which included very high blood pressure, cardiac dysfunction and pulmonary edema. The lab also observed a puncture in the bag.

Ortiz surreptitiously injected IV bags of saline with epinephrine, bupivacaine and other drugs, placed them into a warming bin at the facility, and waited for them to be used in colleagues' surgeries, knowing their patients would experience dangerous complications. Surveillance video introduced into evidence showed Ortiz repeatedly retrieving IV bags from the warming bin and replacing them shortly thereafter, not long before the bags were carried into operating rooms where patients experienced complications. Video also showed Ortiz mixing vials of medication and watching as victims were wheeled out by emergency responders.

Evidence presented at trial showed that Ortiz was facing disciplinary action at the time for an alleged medical mistake made in his one of his own surgeries, and that he potentially faced losing his medical license. (Source)

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) (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

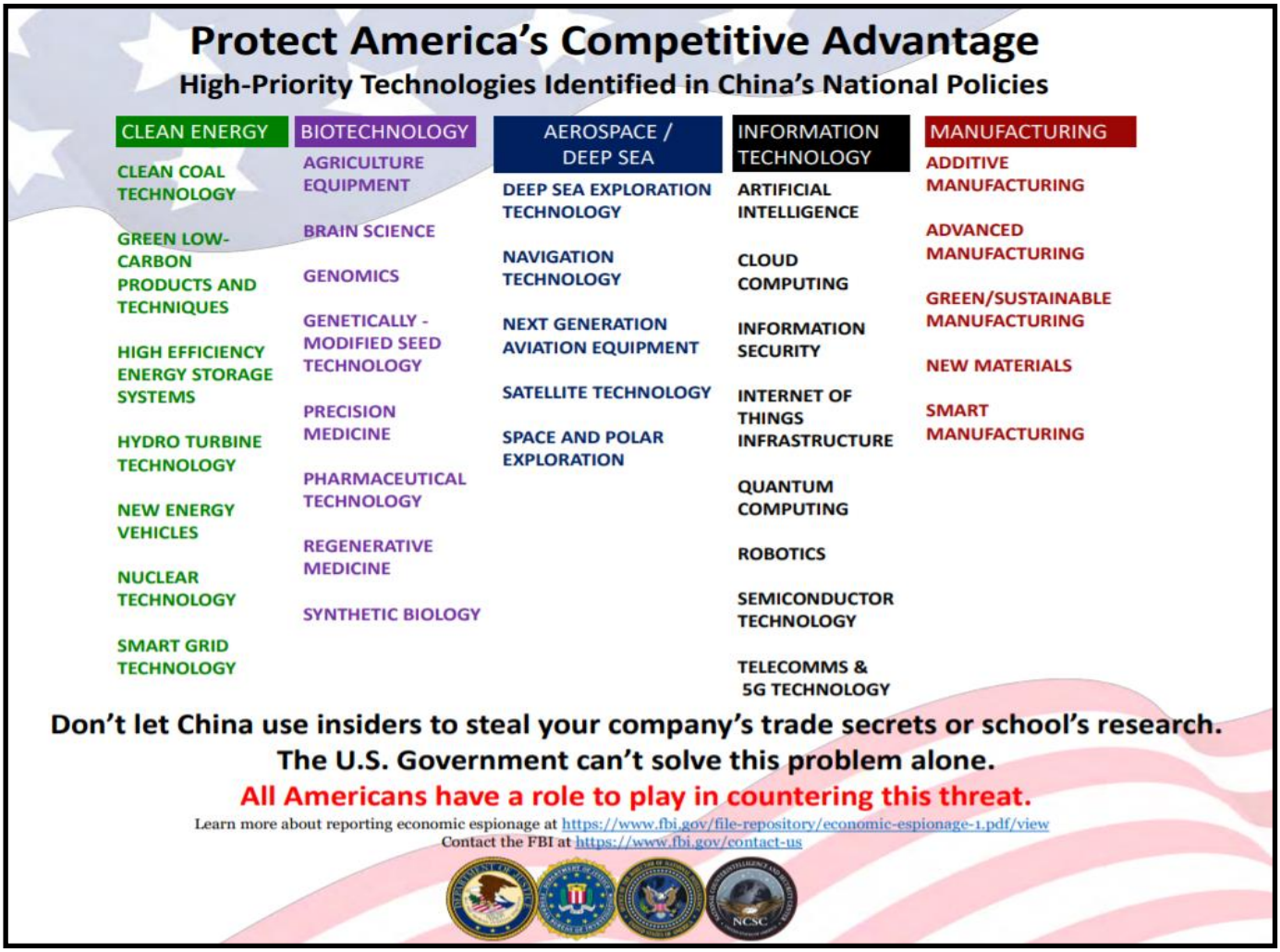
WORKPLACE VIOLENCE TODAY E-MAGAZINE
https://www.workplaceviolence911.com/node/994

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 (**6,000+ Incidents**).

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

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

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

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

INSIDER THREAT INCIDENTS SPOTLIGHT REPORT FOR 2023

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

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

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

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

Incident Posting Notifications

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

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

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

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER / X

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 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, evaluate and optimize an Insider Risk Management (IRM) 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, as well as attended our Insider Threat Investigations - Analysis Training Course and other training courses.

The ITDG are experts at providing guidance to help build Insider Threat Programs (For U.S. Government Agencies, Defense Contractors) and IRM 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 IRM.

ITDG training and consulting services will empower individuals that manage or support IRM Programs, with the comprehensive knowledge, tools and a unified and holistic approach to identify, prevent and mitigate Insider Risks / Threats.

IRM PROGRAM TRAINING & CONSULTING SERVICES OFFERED
Conducted Via Classroom / Onsite / Web Based
TRAINING

- ✓ Executive Management & Stakeholder Briefings For IRM
- ✓ IRM Program Training Course & Workshop / Table Top Exercises For C-Suite, Insider Risk Program Manager / Working Group
- ✓ IRM Program Development, Management & Optimization Training Course
- ✓ IRM Program Evaluation & Optimization Training Course
- ✓ Insider Threat Investigations & Analysis Training Course
- ✓ Insider Threat Awareness Training For Employees'

CONSULTING SERVICES

- ✓ Insider Risk - Threat Vulnerability Assessments
- ✓ IRM Program Maturity Evaluation, Gap Analysis & Strategic Planning Guidance
- ✓ Insider Threat Detection Tool Gap Analysis & Pre-Purchasing Guidance / Solutions
- ✓ Data Exfiltration / Red Team 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 675 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, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more.
(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