INSIDER THREAT INCIDENTS REPORT
FOR
December 2025

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

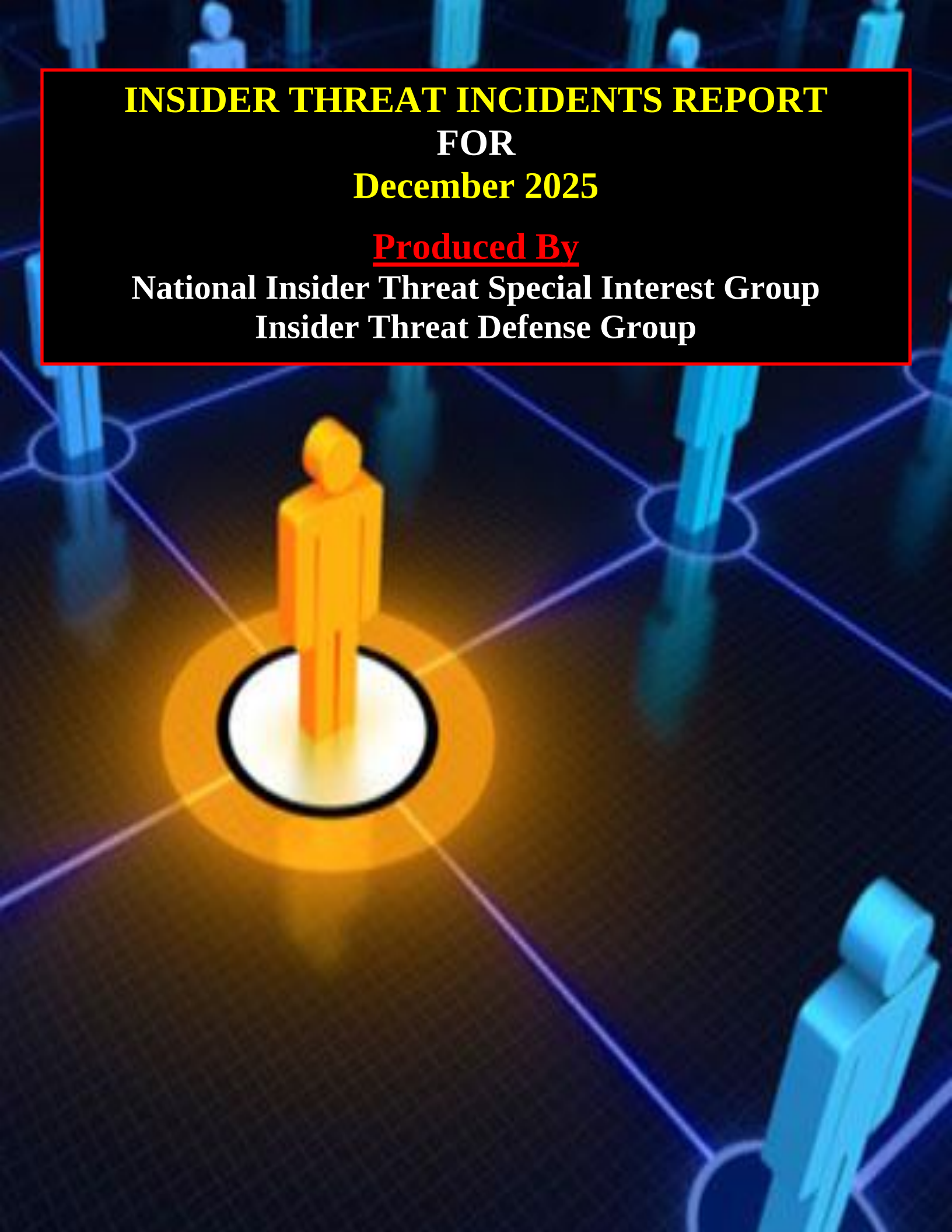


TABLE OF CONTENTS

INSIDER THREAT INCIDENTS OVERVIEW

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 **6,700+** 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 is 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 hundreds of thousands of dollars, maybe million 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 23** 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 DECEMBER 2025

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

South Korean Company Data Breach Caused By Employee Exposed Information On 34 Million Users / Company Must Compensate $1.1 BILLION To Affected Users - December 28, 2025

South Korean online retail giant Coupang said it will offer 1.69 trillion South Korean won ($1.17 billion) in compensation to 34 million users affected by a massive data breach disclosed last month.

The company said in a statement that it planned to provide customers with purchase vouchers totaling 50,000 won for various Coupang services. Former customers who closed their Coupang accounts following the data breach are also eligible to receive the vouchers.

Harold Rogers, interim CEO for Coupang Corp., described the move as a "responsible measure for our customers," and said the company would "fulfill its responsibilities to the end."

The data breach, which was revealed on Nov. 18, 2025 led to the resignation of CEO Park Dae-jun earlier this month.

Coupang founder Kim Bom said in a separate statement that the company had failed to communicate clearly from the outset of the incident. The U.S.-based chairman acknowledged his apology was "overdue," explaining that he initially believed it was best to communicate publicly and apologize only after all the facts were confirmed.

Kim added that the company has recovered all the leaked customer information through cooperation with the government, as well as the storage devices belonging to a suspect behind the data breach.

He also said the customer information stored on the suspect's computer was limited to 3,000 records and that it was not distributed or sold externally.

As the police continued their investigations in Coupang's offices, they uncovered that the primary suspect was a 43-year-old Chinese national who was a former employee of the retail giant. The employee had joined Coupang in November 2022, and was assigned to an authentication management system and left the firm in 2024. He is believed to have already left the country. (Source)

GEOPOLITICAL PROBLEMS AND PROTESTS BY EMPLOYEES

No Incidents To Report

IN DEPTH RESEARCH CONDUCTED ON SIDER THREATS

Data On Insider Threats: What 1,000+ Insider Threat Incidents Reveal - December 2025

Security analyst Michael Robinson spent 14 months reviewing 15,000 legal filings to uncover who malicious insiders really are, how they operate, and why traditional detection models keep missing them.

Robinson distilled insider threats down to 1,000 instances of misconduct and real-world cases where trusted employees turned their access into a weapon.

Robinson's research draws from open US court records across 84 federal districts, Robinson discovered a surprisingly broad distribution of insider incidents spanning over 75 industries, including IT, finance, manufacturing, government, and healthcare. But what surprised him most wasn't where the crimes occurred, it was who committed them.

Who Are Malicious Insiders?

One-quarter of the malicious insiders were top executives. "These were senior people, vice presidents, presidents with trusted with access to the company's most valuable data," he says. "That's a lot of foxes in the henhouse."

Even more unsettling, nearly 20% were high-performing employees who had been promoted, sometimes multiple times.

The research also dismantles another common assumption: that the danger ends when an employee departs. "Over half of the insiders in these cases quit voluntarily," Robinson explains. "They weren't fired — they just left of their own accord. But many came back to do harm after they were gone."

Ex-employees often retained more access than companies realized, with cloud tools, shared passwords, and remote access systems outside corporate single sign-on environments.

Collusion compounds the problem. In 31% of cases, insiders worked in pairs or small groups. (Source)

U.S. GOVERNMENT

2 U.S Government Contractors Arrested For Conspiring To Destroy Government Databases After Termination - December 3, 2025

Brothers Muneeb and Sohaib Akhter, both 34, of Alexandria, Virginia, were indicted on Nov. 13, 2025 for conspiring to delete databases used to store U.S. government information.

Both men were federal contractors. Following the termination of their employment, the brothers allegedly sought to harm the company and its U.S. government customers by accessing computers without authorization, issuing commands to prevent others from modifying the databases before deletion, deleting databases, stealing information, and destroying evidence of their unlawful activities.

On or about Feb. 18, Muneeb Akhter deleted approximately 96 databases storing U.S. government information. Many of these databases contained records and documents related to Freedom of Information Act matters administered by federal government departments and agencies, as well as sensitive investigative files of federal government components.

Muneeb Akhter also allegedly obtained information from the U.S. Equal Employment Opportunity Commission without authorization after he was fired from the contractor. He is further alleged to have stolen copies of IRS information stored on a virtual machine, including federal tax information and other identifying information of at least 450 individuals. (Source)

USDA Employee Sentenced To Prison For Role In $66 Million+ Food Stamp Fraud And Bribery Scheme - December 22, 2025

Arlasa Davis was sentenced to prison for her role in a sprawling fraud and bribery scheme that generated over $66 million in unauthorized transactions under the Supplemental Nutrition Assistance Program (SNAP"), also known as food stamps.

Davis worked within the USDA division responsible for identifying SNAP fraud. She abused her privileged access to federal systems to sell hundreds of Electronic Benefits Transfer (EBT) license numbers to co-conspirators.

Davis photographed handwritten lists of license numbers intended for qualifying stores with her personal cellphone and funneled them to an intermediary who sold them to co-conspirators, who in turn used those license numbers to fraudulently obtain EBT terminals for stores that were not authorized by the USDA to process SNAP transactions. In return, Davis received substantial bribes that were disguised in communications as, among other things, "birthday gifts" and "flowers."

Davis was ordered to forfeit $48,470 and pay restitution of $36 million. (Source)

Former U.S. Government Contractor Employee Charged For Misleading Government Customers About The Security Posture Of Cloud Product Offered By The Company - December 12, 2025

From March 2020 to November 2021, Danielle Hillmer allegedly obstructed federal auditors and falsely represented that an Accenture cloud platform for federal use had required security controls in place.

Accenture said in a 2023 financial filing that the Justice Department was investigating "whether one or more employees provided inaccurate submissions to an assessor who was evaluating on behalf of the U.S. government an AFS (Accenture Federal Services) service offering and whether the service offering fully implemented required federal security controls."

"As previously disclosed in our public filings, we proactively brought this matter to the government's attention following an internal review.

We have cooperated extensively with the government's investigation and continue to do so," an Accenture spokesperson told Nextgov/FCW. "We remain dedicated to operating with the highest ethical standards as we serve all our clients, including the federal government."

Although the platform was marketed as secure for agencies, Hillmer "concealed the platform's noncompliance with security controls under the Federal Risk and Authorization Management Program (FedRAMP) and the Department of Defense's Risk Management Framework," a Justice Department press release says.

FedRAMP is the U.S. government framework for assessing and monitoring the security of private sector cloud services used by federal agencies. Misrepresenting systems' security to the government can be dangerous for agencies' cyber posture because the compliance check helps determine if a product is safe to operate in federal environments.

The DOD Risk Management Framework is similar to FedRAMP, but it applies to military information systems, rather than commercial cloud services used in civilian agencies.

Prosecutors say Hillmer tried to sway and impede independent assessors during mandatory audits in 2020 and 2021 by hiding security gaps and directing others to mask the system's real condition during tests and demos.

She is also accused of giving the Army false information to persuade it to sponsor the platform for a DOD authorization. The charges say Hillmer submitted and directed colleagues to submit authorization documents to assessors that she knew included materially false statements to secure and retain government approvals to operate.

In June 2020, an outside firm that assessed security documentation for the system warned that it wasn't ready for elevation because over 100 security controls were not yet implemented, it adds. But a month later, she still approved the submission to government auditors.

Cyber-related procurement fraud is a major enforcement area for federal prosecutors, who in recent years have pursued contractors accused of overstating their compliance with government-mandated security requirements.

Contractors can profit from these schemes by winning federal business they aren't qualified for, avoiding costly remediation work and preserving lucrative business deals that depend on maintaining the appearance of compliance with strict cybersecurity standards. (Source)

Puerto Rico Department Of Labor Employee And 7 Others Charged For $619.000+ Insurance Fraud Scheme - December 19, 2025

A Federal Grand Jury in the District of Puerto Rico returned an indictment charging 8 women with engaging in fraud scheme to obtain unemployment compensation from the Puerto Rico Department of Labor (PRDOL) totaling $619,923 and to make kickback payments to a public official.

According to the indictment, the defendants conspired to submit false information in order to fraudulently obtain unemployment compensation from the PRDOL. This was done by using false personal identifying information, using identifying information of other individuals, and providing false information related to past employment history.

Luz Garay-Osorio, using her position as an employee of PRDOL, made changes in the PRDOL system to make family members eligible to receive unemployment benefits, Pandemic Unemployment Assistance, and Disaster Unemployment Assistance.

Garay-Osorio also used her position as a PRDOL interviewer to file fraudulent claims, create false work history, change historical changes, and make monetary and non-monetary determinations. In addition, Garay-Osorio submitted fraudulent claims using other individuals' identities and caused benefits to be paid to co-conspirators, including family members. (Source)

United States Geological Survey Employee Sentenced To Prison For Misusing Government Charge Card For $1.1 Million+ In Charges Over 15 Year Span - December 2, 2025

James Montoya worked as a federal employee at the United States Geological Survey (USGS) office in Lakewood, Colorado.

USGS is part of the United States Department of the Interior (DOI). During a routine initiative to identify misuse, DOI identified numerous questionable transactions on Montoya's government charge card. An investigation revealed that Montoya successfully concealed improper purchases for years by submitting altered receipts, and fictitious invoices and other documentation to USGS claiming that these purchases were for IT-related items or services.

In fact, the defendant did not provide any IT-related items or services to USGS and many of these purchases were for personal items including, but not limited to, vintage and collectible toys as well as car parts.

The alleged actions defrauded the government of approximately $1,122,009.47 over approximately fifteen years beginning around December of 2008 and continuing through at least November 2023. (Source)

U.S. Postal Service Employee Pleads Guilty To Receiving $1.5 Million In Bribes For Contracts - December 4, 2025
Zechariah Yi, is a former United States Postal Service (USPS) employee.

Zechariah Yi, 52, was indicted in March 2025 for his role in accepting payments related to USPS service contracts awarded to certain trucking companies. On November 2, 2025 Yi pled guilty to one count of receiving a bribe by a public official.

Yi admitted that, while working as a Senior Network Operations Analyst for the USPS, he solicited and received approximately $1.5 million in kickbacks from the owners and associates of three trucking companies in exchange for Yi's agreeing to help the trucking companies obtain USPS service contracts. The USPS service contracts awarded to the three trucking companies paid the companies a total of approximately $15 million.

Yi is the fourth defendant to plead guilty as part of this bribery scheme. Previously, another USPS employee, Tai Rho, and the owners of two trucking companies, Wan Jin Yoon and Hong Jin Yoon, each pled guilty to one count of Conspiracy to Commit Honest Services Wire Fraud for their involvement in the bribery scheme. They each face up to five years in federal prison. All three are set for sentencing in early 2026. (Source)

U.S. Postal Service Employee Sentenced To Prison For Role In Stealing $660,000 Worth Of Checks & Credit Cards From Mail / Used Funds For Luxury Lifestyle - December 8, 2025
Mary Magdamit, formerly worked as a letter carrier for the United States Postal Service in Torrance, California.

From at least 2022 until July 2025, Magdamit stole mail containing checks, personal identifying information (PII), and debit and credit cards. She then activated the stolen bank-issued cards online, used the cards to make purchases, and sold some stolen cards to her co-conspirators.

Law enforcement searched Magdamit's apartment in December 2024, and seized 133 stolen credit and debit cards,16 U.S. Department of Treasury checks, and a loaded, un-serialized Glock-clone, with an extended 27-round magazin. Agents also discovered luxury goods purchased with cards she stole from the mail.

Magdamit used the funds to take international trips and buy luxury goods, and then flaunting the cash on Instagram. Magdamit was ordered to pay $660,200 in restitution. (Source)

U.S. Postal Service Employee Sentenced To Prison For Role In Stealing $285,000+ Of Checks - Debit Cards From Mail / Used Funds For Personal Reasons - December 9, 2025
Kierra Blount, at times while employed by the U.S. Postal Service in Stamford, Connecticut, stole mail and obtained stolen mail for the purpose of obtaining checks that were payable to other individuals.

In approximately November 2021, Blount opened a bank account using the name and social security number of an individual without the identity theft victim's knowledge.

Blount and others fraudulently changed the payee names on stolen checks to the name of the identity theft victim, forged the victim's signature on the back of the checks, and deposited them into the bank account Blount opened.

From November 2021 until the account was closed in April 2022, Blount and others deposited approximately $156,000 in fraudulent checks into the account. Some check deposits were reversed by the bank, and Blount and others used approximately $81,000 for their own purposes.

On June 20, 2023, investigators conducted a court-authorized search of Blount's residence and seized a significant amount of stolen mail and other items related to this scheme, including debit cards in the names of other individuals, checks totaling more than $285,000, and sheets of paper containing personal information of other individuals, including names, dates of birth, addresses, email addresses, and security question answers. Subsequent analysis of cell phones seized from Blount on that date revealed images of stolen checks, personal identifying information for more than 50 individuals, and communications using the Telegram app with unknown individuals involved in the scheme. (Source)

U.S. Post Office Station Manager Sentenced To Prison For Stealing $81,000+ Of Stamps - December 1, 2025

Emilio Chirico, 57, admitted that between January 2021 and March 2023, he stole $81,553.94 in stamps from the DeWitt Post Office and falsified postal records to conceal the theft of the stamps. Chirico had been the station manager at the DeWitt Post Office in New York since March 2012.

Chirico must pay a total of $81,553.94 in restitution and a $5,500 fine. (Source)

U.S. Postal Service Employee Charged For $51,000+ Of Workers' Compensation Fraud - December 19, 2025

In 2012, Graciela Venegas began receiving workers' compensation benefits for an injury she sustained in the performance of her Postal Service duties. Venegas claimed her spouse as a dependent, which entitled her to receive augmented benefits. The couple divorced in 2013, and the ex-spouse then passed away in 2014.

Venegas fraudulently continued to claim the spouse as a dependent after the divorce and death. From 2013 to 2024, while employed by the Postal Service, Venegas fraudulently received monthly augmented workers' compensation payments amounting to an additional 8 and 1/3 percent of her pre-injury monthly pay, the indictment states. In total, Venegas fraudulently pocketed $51,776 in augmented benefits to which she knew she was not entitled, the indictment states. (Source)

U.S. Postal Deliveryman And 2 Others Charged With Bribery & Drug Trafficking Through The U.S. Mail - December 4, 2025

From January 2022 until April of 2024 the defendants conspired to distribute over 100 kilograms of marijuana through the United States Postal Service (USPS).

Defendant Héctor Melvin Candelaria-Carrero, served as a USPS City Carrier in Isabela, Puerto Rico. While engaged in his official duties, Candelaria-Carrero diverted, delayed and stole USPS parcels and provided the diverted and stolen mail to defendants Carlos Nadín Nieves-Pastrana, and José Manuel Muñoz-Torres in exchange for bribe payments.

At times, Candelaria-Carrero took photos of specific parcels with his personal phone. Using the assigned USPS scanner device, he scanned the photos taken on his personal phone at the correct delivery address.

Rather than deliver the parcels at the delivery addresses, Candelaria-Carrero diverted the parcels to other locations and hid the locations of the diverted and stolen mail from the USPS.

Candelaria-Carrero used his private cellular number, WhatsApp messages and phone calls to communicate with Nieves-Pastrana and Muñoz-Torres and to exchange bribe payments and the diverted or stolen parcels, including parcels containing controlled substances. (Source)

U.S. Postal Service Emplyee Convicted For Stealing Cash And Gift Cards From Mail - December 15, 2025

Shannon Littlefield, 29, stole cash and gift cards from greeting cards entrusted while working at the Auburn Post Office in Maine Littlefield worked as a Service and Distribution Clerk from May 2016 through March 2025.

In March 2025, Littlefield was observed on surveillance footage on three different dates removing mail from mail bins and placing it under her clothing.

When investigators with the U.S. Postal Service Office of Inspector General questioned Littlefield about her conduct, she confessed that she had been stealing mail for approximately eight months. Littlefield admitted that she would open greeting cards and steal cash or gift cards enclosed in the greeting cards. (Source)

National Park Service Employee Sentenced To Probation For Stealing $249,000 Of Funds For Camping & Cave Fees Over 4 Years - December 15, 2025

U.S. District Judge Audrey G. Fleissig on Monday sentenced a former employee of the National Park Service to five years of probation and ordered her to repay $249,000 in campsite and tour fees that she stole from 2019 to 2023. Some of the cash she deposited it into her own account.

Lisa Figge was a supervisory visitor use assistant at the Ozark National Scenic Riverways in Missouri Figge's job duties included collecting fees for guided tours of Round Spring Cave and collecting cash in envelopes placed in metal drop boxes at campsites known as "Iron Rangers." From 2019-2023, Figge stole some of the cash and deposited it into her own account.

On Aug. 28, 2023, Figge was caught on video counting cash and stealing $1,200. Figge was then spotted stopping at her own bank before traveling to the bank that the Park Service used. In an interview with investigators later that day, Figge admitted stealing money from the cave tour program and the fee collection program, including directly from Iron Rangers.

Figge said she altered records and created a false deposit report to hide her crime. Figge told investigators that she did not keep records of how much money she had stolen, but the parties agreed that the amount of provable loss to the Park Service exceeded $200,000. Figge has already repaid $100,000 of the money. (Source)

Department Of Energy Engineer Settles Claims Of Secretly Working Air Force Contractor Jobs & Collecting $165,000+ - December 3, 2025

Jose Nieves was employed as an engineer at DOE's Sandia Field Office.

Between April 2021 and September 2021, he allegedly took a second job with Air Force contractor Pacific Architects and Engineers (PAE) while still working full-time at DOE.

After leaving PAE, he allegedly secured another position with Arctic Slope Regional Corporation (ASRC) from September 2021 through July 2022, again while maintaining his DOE job.

The government's investigation revealed that Nieves allegedly lied to get these contractor positions. He reportedly told PAE he had retired from DOE when applying for that job. Later, when applying to ASRC, he allegedly claimed his DOE employment had ended. In reality, he kept working at DOE during both contractor jobs.

To maintain the deception, Nieves allegedly submitted false timesheets to both employers during his dual employment. Investigators found he filed 19 fraudulent timesheets with PAE, 24 with ASRC, and 33 with DOE, claiming to work full-time hours at both jobs simultaneously. This scheme allegedly allowed him to collect two government paychecks for overlapping work hours.

The Air Force contractors paid Nieves based on these false timesheets and then sought reimbursement from the government, resulting in improper payments of taxpayer funds. Under the settlement agreement, Nieves will pay the United States $165,000, which includes $156,799.22 in restitution. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Former DoD Employee Pleads Guilty To Removing Classified Documents From Her Office - December 15, 2025

Ewa Ciszak was arrested in June 2025 after her Huntsville home was searched due to reports of her removing secret documents. She reportedly took classified documents home from the Missle Defense Agency for over six months. During the search, documents were recovered from a backpack in her car and her home.

At the time, Ciszak told investigators that she was using the documents to work on a presentation for her job.She was charged with Knowlingly Removing and Retaining Documents and Materials. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

TSA Security Officer Charged With Fraudulently Obtaining $47,000+ Of Pandemic Unemployment Assistance - December 17, 2025

Ismael Rosado was employed full-time as a TSA Security Officer at Boston Logan International Airport from November 2018 through October 2021.

It is alleged that, between May 2020 and September 2021, Rosado submitted an application seeking PUA and weekly certifications claiming he was unemployed and making no income. Based on the misrepresentations in the application and weekly certifications, Rosado received $47,526 in unemployment benefits to which he was not entitled. (Source)

California Highway Patrol Auto Technician Arrested For Role In Stealing Vehicle Components And Re-Selling - December 23, 2025

An employee with the California Highway Patrol was arrested for embezzlement after being accused of stealing vehicle components from the agency, the CHP exclusively told NBC4 Investigates Tuesday.

Dareth Chau, a CHP auto technician, was arrested following an extensive investigation into an alleged theft scheme," the CHP said.

Chau stole the vehicle components then sold them to his co-conspirator, Mario Castellano. CHP investigators believe Castellano then resold the stolen parts or used them on vehicles that he sold. (Source)

Correctional Officer Sentenced To Prison For Smuggling Narcotics Into Jail By Hiding In Waistband - December 30, 2025

Tyrell Wallace was a correctional officer at the Dyer County Jail in Tennessee. Wallace reported to work on October 24, 2024. Investigators stopped Wallace and announced an administrative search. Inside Wallace's waistband, investigators recovered 53 grams of actual methamphetamine with a purity level of 100%, 165 grams of marijuana, 26 grams of fentanyl, 3 grams of crack cocaine, 8 Suboxone strips, and a Motorola cellular telephone.

Investigators then searched Wallace's vehicle where they recovered a loaded 9mm handgun and 40 rounds of ammunition. During a post-arrest interview, Wallace confessed that he planned to introduce the narcotics to inmates. Investigators then sought a search warrant for Wallace's cellphone which revealed it was the third time he delivered controlled substances to the jail. (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

State Unemployment Insurance Agency Employee Sentenced To Prison For Stealing $250,000 Of Unemployment Insurance Benefits - December 4, 2025

Timeka Johnson, a former employee of the State of Michigan Unemployment Insurance Agency and her former romantic partner (Ray Anthony Eddington) were sentenced to prison for their roles in an unemployment insurance fraud conspiracy.

Johnson used her insider access to fraudulently process claims in the names of third parties. As a result of the conspiracy, over $250,000 in fraudulent unemployment assistance payments were made by the State of Michigan. (Source)

Social Services Case Worker Pleads Guilty to Stealing Over $100,000+ From Benefits Program / Used Funds For Personal Benefit - December 12, 2025

Between January 2021 to January 2024,Shermeca McCrary using her position and privileges as a North Carolina Department of Social Services case worker, unlawfully accessed the SNAP accounts of qualified individuals and converted $102,000 in government funds for her own personal benefit and use.

McCrary was ordered to pay a forfeiture money judgment of $102,000.00. (Source)

County Welfare Benefits Employee Arrested For Improperly Using Other People's Identities to Steal $40,000+ Of Benefits - December 12, 2025

Between December 2020 and April 2025 Leticia Mariscal improperly used county databases to which she had access through her job to obtain identifying information for individuals who were elderly or deceased.

She then secretly approved these individuals to receive CalFresh benefits, printed EBT cards in their names with the benefits deposited thereon and spent the proceeds. Altogether, Mariscal used the identities of more than 15 people to steal benefits totaling more than $40,000. She was placed on leave earlier this year when her scheme was discovered. (Source)

Senior Vice President Of Atlanta Housing Authority Charged With $36,000+ Of Housing Assistance Fraud & $27,000+ Of COVID Relief Fraud - December 22, 2025

Since April 2017, Tracy Jones has served as Senior Vice President over the Housing Choice Voucher Program at the Atlanta Housing Authority. She oversaw one of the largest Section 8 programs in the country. The U.S. Department of Housing and Urban Development funds Section 8 programs, including rental assistance payments to landlords on behalf of low-income families and individuals. Section 8 funds are limited, and there is often a long waiting list of low-income families seeking acceptance into the program. Housing authority staff are generally prohibited from receiving Section 8 payments for their own properties, and Section 8 landlords are typically prohibited from leasing to their own family members.

Jones allegedly defrauded the program by using a series of falsified forms to have her family members admitted to the Section 8 program and then to receive Section 8 payments for them to live in her own rental house. To conceal her identity, Jones allegedly used a fake name and a shell business entity to execute housing authority documents. As a result, she improperly obtained more than $36,000 of Section 8 funds. Jones then allegedly obstructed subsequent investigations by submitting a false affidavit and convincing friends to lie and present false documents on her behalf.

At the same time, Jones allegedly used her shell business and another business to collect more than $27,000 from the U.S. Small Business Administration's COVID-19 pandemic relief programs, falsely claiming that the businesses were functioning, had multiple employees, and received over $56,000 of gross revenues in 2019. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

University Assistant Professor Sentenced To Prison For Embezzling $412,000+ - December 4, 2025

Gary Grajales-Reyes, MD-PhD, is a former assistant professor who embezzled $412,163 from the Washington University School of Medicine.

The judge also ordered Grajales-Reyes to repay the money. Federal law enforcement has already seized a substantial quantity of collectible trading cards from Grajales-Reyes' laboratory that he bought with some of the funds.

Grajales-Reyes admitted submitting 73 false requisition requests to WashU Medicine for 761 different pieces of computer equipment, falsely claiming that it was for the research laboratory that he directed.

Once he received the equipment at his lab, Grajales-Reyes sold some of the computer equipment through his personal eBay site and some to an Amazon-based third-party seller. He used the money obtained by selling the computer equipment for his own personal expenses. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

Union President Arrested For Stealing $290,000+ After He Was Voted Out Of Office / Used Funds Travel & Renovating A Property - December 1, 2025

Between 2003 and 2023, Carbone served as the President of United Federation of College Teachers Local 1460, the union representing faculty members at the Pratt Institute in Brooklyn, New York.

As alleged in the indictment, Carbone stole over $290,000 from the Local between 2011 and 2023, when he was voted out of office. Carbone used the money for his personal expenses, restaurants and travel, and buying and renovating a property in Athens. (Source)

BANKING / FINANCIAL INSTITUTIONS

Bank Branch Manager Convicted Of Embezzling $655,000 / Deposited Funds Into Her Bank Accounts - December 17, 2025

Starting in June 2021, Brooke McDonough stole cash from the ATM machines and vault inside the branch she managed. She then deposited most of the cash she stole into her personal bank accounts, using different ATMs at multiple bank branches.

In total, between June 2021 and February 2022, McDonough embezzled $655,000 from the branch she managed and deposited or spent approximately $645,000 in cash during the same time period. McDonough broke down her ATM cash deposits into smaller amounts to avoid having the banks file Currency Transaction Reports for deposits of over $10,000 in cash. (Source)

Bank Vice President Sentenced To Prison For $590,000+ Loan Fraud Scheme / Used Funds For Luxury Lifestyle - December 8, 2025

Kaylee Lunn admitted that while she was vice president of commercial lending at the Wichita Falls branch of First Capital Bank in Texas, she accessed and unlawfully used the personal and business financial information of certain bank customers to apply for a series of four fraudulent PPP loans and a commercial loan in late 2020 through mid-2021.

Lunn admitted that she used false or inflated income and payroll expense figures and diverted loan proceeds totaling more than $276,000 to bank accounts she controlled, all without the customers' knowledge or consent.

Lunn applied for and received more than $140,000 in fraudulent PPP loans falsely reflecting the business entities as her husband's.

Throughout this time period, Lunn also made failed attempts to obtain several Economic Injury Disaster loans of over $890,000, which were ultimately rejected because they were associated with fraudulent information.

According to plea documents, Lunn spent thousands of dollars of the fraudulently-obtained loan proceeds on her personal and lifestyle expenses.

Lunn was ordered to pay restitution of $573,444 to the Small Business Administration and more than $19,000 to her former employer, Prosperity Bank. (Source)

Bank Of America Employee Arrested For Stealing $500,000+ From Woman With Disabilities - December 24, 2025

Mario Martinez, was arrested and faces several charges after a co-worker reported that he was stealing funds from a disabled woman in southwest Miami-Dade County.

Martinez, 40, was accused of stealing over $500,000 from a woman with disabilities who had received a large inheritance.

The victim a 47 year-old woman has been with Bank of America for about 20 years. She suffers from a chronic condition where she is unable to walk and requires full-time care. Martinez learned from the woman that she had inherited a large amount of money and needed help managing her finances. Martinez allegedly told her he was a financial adviser who could help her invest and manage her money. Martinez had known her since 2016; however, he was not a financial adviser.

Martinez began funneling her inheritance funds into his own account from April 2024 to December 2024, and created a joint account in both their names without her permission. He did this after she lent Martinez $120,000 in early 2023 after he told her he had incurred a large debt. (Source)

Credit Union Customer Service Employee Sentenced To Prison For Stealing $345,000+ From Credit Union Customers - December 4, 2025

Between May and August 2022, Aneicia Ford worked out of her home as a contact center employee who helped customers with account issues. In that role, she had access to personally identifying information about customers of the credit union.

Although Ford's role in the conspiracy was relatively simple, she nonetheless independently analyzed the victims' accounts to ensure a specific account would be a fruitful and viable target for the conspirators.

Only Ford had access to information such as the amount of funds available, or the age or profession of an individual victim. The first account takeover in the scheme occurred just days after Ford completed her training to be a customer service representative for the credit union.

The personally identifying information Ford stole was distributed by 23-year-old codefendant Dangelo Roberts, who with other conspirators used it to access and steal from customer accounts.

Using the stolen account information, Roberts provided other conspirators with false IDs and used them to get debit cards and to make withdrawals from the victims' accounts, often at the credit union's branches. After obtaining increases to the ATM withdrawal limits, the conspirators obtained as much as $25,000 in cash.

The conspirators would also spend victims' funds by ordering cashier's checks or purchasing postal money orders that they made payable to other conspirators or their associates. They used their illegal access to transfer money between accounts and check balances on accounts.

In all, the scheme stole approximately $345,014 from accounts at the victim credit union. The victim credit union suffered that loss, making all the account holders whole. (Source)

Truist Bank Employee Sentenced To Prison For Stealing $200,000 From 70 Customer Accounts / Used Funds For Clothing, Travel, Etc. - December 2, 2025

In 2023, Ahshah Martin began improperly using her access to Truist computer systems to gather Truist account holders' banking information. Then, she initiated fraudulent debits and withdrawals from these accounts for her own benefit. For instance, Martin repeatedly initiated payments from customer bank accounts to a child support payment processor, through which Martin paid herself. In all, Martin used her access to sensitive customer financial information to steal $195,000 from at least 70 separate Truist customer accounts.

Martin stole from the Truist accounts of individuals and entities, including multiple churches, a children's museum, an eye tissue bank non-profit organization, manufacturing and construction companies, a small business making customized holsters, and the North Carolina Wing of the Civil Air Patrol.

Martin spent stolen funds on cosmetic products, clothing, travel expenses, dining, and at a hookah bar.

On April 15, 2024, Martin was terminated by Truist. Despite repeated attempts to retrieve her Truist laptop, Martin retained access to her work computer. To conceal her wrongdoing and prevent the return of her Truist laptop, Martin faked her own death. On April 17, 2024, in response to an email from Truist asking for the computer, Martin responded, "Sorry to inform you, she has passed away." (Source)

Former Bank Of Hawaii Teller Indicted For Embezzling $40,000+ From Customers - December 14, 2025

A 24-year-old former Bank of Hawaii teller pleaded not guilty to charges she allegedly embezzled more than $40,000 from bank customers, including two elderly customers.

Alohi K. Kaupu-Grace embezzled $44,000 from customer accounts and falsified the customers' signatures on cash withdrawal slips and cashier's check purchase slips. In one of those cases, the victim contacted police to report he received a text from his credit card company alerting him of a fraudulent charge made to his account in excess of $750.

Detectives from Hawaii Police Department's East Hawaii Criminal Investigation Section reportedly determined Kaupu-Grace was responsible for the unauthorized transaction and had obtained the victim's personal confidential information while working for Bank of Hawaii." (Source)

Former President Of Failed Oklahoma Bank Indicted For Bank Fraud - December 4, 2025

Danny Seibel, served as the President and Chief Executive Officer of the First National Bank of Lindsay from in or about February 2007 until his termination in September 2024.

Seibel also held other management roles at the bank during that time, including Chief Financial Officer and Bank Secrecy Act Officer.

Seibel caused the bank to issue loans to certain customers, many of whom were his personal friends and neighbors, that the borrowers never repaid. Seibel then allegedly manipulated the bank's records and falsified various bank reports to falsely overstate the performance of the loans, including by using new loans or transfers of the bank's own funds to cover overdrafts of outstanding loans.

Seibel frequently modified bank records to conceal this activity from the Office of the Comptroller of the Currency (OCC), which was the bank's federal regulator, as well as from the bank's Board of Directors and others.

During the summer of 2024, when the OCC was conducting an onsite examination at the bank, Seibel allegedly provided OCC staff with a false document that concealed hundreds of changes that Seibel had made to loan data. The indictment also alleges that Seibel failed to implement an anti-money laundering program at the bank as required by the Bank Secrecy Act.

For example, Seibel allegedly failed to file any suspicious activity reports on his own fraudulent scheme, and he advised Bank customers to make cash deposits below $10,000 to avoid relevant reporting requirements. (Source)

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

Harvard Medical School Morgue Manager And Wife Sentenced To Prison For Trafficking Stolen Human Remains - December 16, 2025

From 2018 through at least March 2020, Cedric Lodge participated in the sale and interstate transport of human remains stolen from Harvard Medical School morgue, located in Boston, Massachusetts.

Cedric Lodge, who was then employed as the manager of the Harvard Medical School Morgue, removed human remains, including organs, brains, skin, hands, faces, dissected heads, and other parts, from donated cadavers

after they had been used for research and teaching purposes but before they could be disposed of according to the anatomical gift donation agreement between the donor and the school. Cedric Lodge took the remains without the knowledge or permission of his employer, the donor, or the donor's family, and transported the remains to his home in New Hampshire. After he and his wife Denise Lodge sold the remains, they would ship the remains to the buyers in other states or the buyer would take possession directly and transport the remains themselves. Remains stolen and sold by the Lodges were transported from the morgue in Boston to locations in Salem, Massachusetts, New Hampshire, and Pennsylvania. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

10 Former Samsung Employees Arrested For Stealing Trade Secrets And Providing To China Company - December 23, 2025

South Korean prosecutors have arrested 10 former Samsung employees who have allegedly leaked 10-nm DRAM technology to ChangXin Memory Technologies (CXMT). The 10 individuals are accused of breaking the Act on Prevention of Divulgence and Protection of Industrial Technology, better known as the Industrial Technology Protection Act. Of the ten, five are key development personnel, which includes a former executive. Others include section heads responsible for development and research. Prosecutors say that after CXMT's founding in 2016, it recruited executives and key people from Samsung Electronics, which was the only place mass-producing 10-nm DRAM at that time.

The leak allowed CXMT to produce China's first 10-nm DRAM in 2023, with prosecutors arguing that the stolen technology laid the groundwork for the Chinese company's advancements in HBM. CXMT reportedly began mass production of HBM2 memory in 2024, and that it's expected to capture as much as 15% of the market, resulting in trillions of losses in Korean Won for both Samsung and South Korea's national economy. This can arguably be seen already as Samsung Electronics' sales declined by about 5 trillion Won last year.

Reports indicate that a Mr. A, a former Samsung executive, was in charge working on 10-nm DRAM technology for CXMT, while Mr. B, a key employee involved with the research on the technology allegedly copied information on DRAM manufacturing.

Mr. B transcribed 12 pages of information manually to avoid detection, especially as semiconductor companies are particularly protective of their information and that copying files from a computer or photographing them with a smartphone could lead to them being caught. (Source)

Insurance Broker Aon Files Lawsuit Against 2 Former Senior Employees For The Theft Of Confidential Information And The Resignation Of 7 Employees - December 15, 2025

The complaint, filed on December 11, 2025 in the United States District Court for the Southern District of New York, is the sixth legal action brought against Howden by rival brokers since July 2025, according to Aon. No findings have yet been made by the court.

The plaintiffs in this month's lawsuit are Aon Risk Services Companies and Aon Risk Services Northeast. The defendants are Anthony Rampersaud, a former Aon managing director with more than 23 years' service, Nancy Montalvo, a former account executive with 26 years tenure at Aon, and Howden US Services.

Aon has alleged that Rampersaud orchestrated a coordinated departure of six Aon colleagues to Howden, while still employed by the broker, breached contractual and fiduciary obligations and attempted to remove large volumes of confidential client and financial data in the weeks before his resignation.

According to Aon's complaint, all seven of its referenced employees resigned on November 25, 2025 within hours of each other, with most resignations supposedly submitted within minutes.
Aon's complaint alleges that in early November 2025, Rampersaud printed documents and saved spreadsheets containing revenue projections, client pipelines and account data in a computer folder labelled "top secret".

Aon further alleges that on November 21, 2025, seven boxes of documents were shipped from its New York office to Rampersaud's home address in New York using Aon's FedEx account.

According to the lawsuit documentation, the boxes contained client schedules of insurance, documents marked 'proprietary and confidential', peer benchmarking data and account revenue information covering more than 80 clients. (Source)

ARTIFICIAL INTELLIGENCE (AI) INSIDER THREATS

The Hidden Legal Minefield: Compliance Concerns And Risks With AI Smart Glasses - December 15, 2025

AI-enabled smart glasses are rapidly evolving from niche wearables into powerful tools with broad workplace appeal, but their innovative capabilities bring equally significant legal and privacy concerns.

Modern smart glasses blend high-resolution cameras, always-on microphones, and real-time AI assistants into a hands-free wearable that can capture, analyze, and even transcribe ambient information around the wearer.

These features from continuous audio capture to automated transcription create scenarios where bystanders (co-workers, customers, etc.) may be recorded or have their conversations documented without ever knowing it, raising fundamental questions about consent and the boundaries of lawful observation.

These core capabilities intersect with consent requirements and note-taking practices under U.S. and state wiretapping and recording laws. In many jurisdictions, recording or transcribing a conversation without the express permission of all participants, particularly where devices can run discreetly in the background, can potentially trigger two-party (or all-party) consent obligations and potential statutory violations.

Likewise, the promise of AI-assisted note taking, where every spoken word in a meeting could be saved, indexed, and shared, brings not just operational benefits but significant legal and business risk.

Understanding how the unique sensing and recording features of smart glasses intersect with these consent and note taking issues is essential for any organization contemplating deployment or allowing these devices to be used in the workplace. (Source 1, Source 2)

AI Adoption Surges While Governance Lags — Report Warns Of Growing Shadow Identity Risk - December 2, 2025

AI/Data Breach, Research: The 2025 State of AI Data Security Report reveals a widening contradiction in enterprise security: 83% of organizations use AI in daily operations, but only 13% have strong visibility into how these systems handle sensitive data. As a result, two-thirds have caught AI tools over-accessing sensitive information, and 23%t admit they have no controls for prompts or outputs.

Produced by Cybersecurity Insiders with research support from Cyera Research Labs, the study reflects responses from 921 cybersecurity and IT professionals across industries and organization sizes.

Autonomous AI agents stand out as the most exposed frontier. Seventy-six percent of respondents say these agents are the hardest systems to secure, while 57 percent lack the ability to block risky AI actions in real time. Visibility remains thin: nearly half report no visibility into AI usage and another third say they have only minimal insight — leaving most enterprises unsure where AI is operating or what data it touches.

Governance structures lag behind adoption as well. Only 7 percent of organizations have a dedicated AI governance team, and just 11 percent feel prepared to meet emerging regulatory requirements, underscoring how quickly readiness gaps are widening. (Source)

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

Man Sentenced To Prison For Fraudulent Scheme That Assisted Foreign IT Workers (Posing As U.S. Citizens) With Obtaining Remote IT Positions With U.S. Companies - December 4, 2025

Minh Vong conspired with others, including William James, a foreign national living in Shenyang, China, to defraud U.S. companies into hiring Vong as a remote software developer. After securing these jobs through materially false statements about his education, training, and experience, Vong allowed James and others to use his computer access credentials to perform the remote software development work and receive payment for that work.

James submitted a fraudulent resume in Vong's name to a Virginia-based technology company for a web application developer position that required U.S. citizenship as a condition of employment. The resume falsely represented that Vong possessed a Bachelor of Science degree and 16 years of experience as a software developer. In fact, Vong did not have a college degree or experience in software development.

On March 28, 2023, Vong participated in an online job interview with the CEO of a Virginia-based company.

Vong verified his identity and citizenship by showing his Maryland driver's license and U.S. Passport.

Following the interview, the Virginia-based company hired Vong and assigned him to work on a contract for the Federal Aviation Administration (FAA) involving a particular software application used by various U.S. government agencies to manage sensitive information regarding national defense matters.

The Virginia-based company provided Vong with a laptop to use in connection with his employment and the FAA authorized Vong to receive a Personal Identity Verification card to access government facilities and systems. Vong installed remote access software on the laptop to facilitate Doe's access to it and conceal his location in China.

Between March 2023 and July 2023, Doe used Vong's credentials to perform the software development work from his location in China. The Virginia-based company paid Vong more than $28,000 in wages for work he performed, portions of which Vong then sent overseas to Doe and other conspirators.

Vong admitted that the Virginia-based company was not the only company he and his co-conspirators defrauded. Between 2021 and 2024, Vong used fraudulent misrepresentations to obtain employment with at least 13 different U.S. companies, who collectively paid Vong more than $970,000 in salary for software development services that were, unbeknownst to them, performed by James or other overseas conspirators. (Source)

LARGE FINES OR PENALTIES THAT HAVE TO BE PAID BECAUSE OF INSIDER THREAT INCIDENTS

No Incidents To Report

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

Employee Of Oil & Gas Trading Company Sentenced To Prison For $1 Million International Bribery And Money Laundering Scheme - December 9, 2025

Glenn Oztemel is a former senior oil and gas trader. He was sentenced to prison for his role in a nearly 8 year long scheme to bribe Brazilian government officials and to launder money to secure business for Arcadia Fuels Ltd. (Arcadia) and Freepoint Commodities LLC (Freepoint), two companies where he worked. He was also fined $300,000.

Oztemel paid over $1 million in bribes to officials at Petróleo Brasileiro S.A. (Petrobras), the Brazilian state-owned oil and gas company, in exchange for inside Petrobras information — including competitor bids and confidential pricing information from other U.S. companies — that gave Arcadia and Freepoint a competitive advantage in winning lucrative fuel oil contracts from Petrobras. (Source)

Restaurant Chains District Manager Sentenced To Prison For Stealing $685,000 By Manipulating Employer's Payroll - December 17, 2025

Javier Ruiz stole $685,376 from his employer, a franchisee of national restaurant chains.

As a district manager, Ruiz supervised a number of restaurants in Idaho, including overseeing payroll. From at least April 2021 through April 2024, Ruiz devised a scheme wherein he manipulated his employer's payroll system, changing the names and other information associated with employee numbers of former employees.

After manipulating the employee numbers, Ruiz entered hours using the numbers that were never worked, causing fraudulent payroll payments to issue. To access and take the fraudulent payroll money, Ruiz used at least three different methods – cashing checks, depositing earnings on fraudulent Rapid Paycards, and direct deposit. (Source)

Employee Sentenced To Prison For Embezzling $500,000 - December 5, 2025
John Laakso was a former Engineering Manager for the local company.

Laakso defrauded his employer of nearly $500,000. He did so by secretly awarding lucrative contracts to his own pass-through companies, both for services that Laakso never provided, and for goods and services that Laakso secretly billed to his employer at a fraudulent rate. (Source)

Employee Convicted For Embezzling $130,000+ - December 5, 2025
Ashley Hymel used a company credit card to embezzle funds from her employer, where she was an executive assistant. Hymel embezzled at least $130,663.92. Hymel agreed to pay the entire amount back to company. (Source)

EMPLOYEES' WHO EMBEZZLE / STEAL MONEY BECAUSE OF FINANCIAL PROBLEMS, FOR PERSONAL ENRICHMENT, TO LIVE ENHANCED LIFESTYLE OR TO SUPPORT GAMBLING ADDICATIONS

Company Chief Financial Officer Pleads Guilty To Embezzling $4.5 Million / Used Funds To Pay Credit Cards, Down Payment For Vacation Property, Etc. - December 18, 2025
From about March 2022 to November 2024, Jonathan Leissler, 44, of Stow, Ohio, worked at an industrial supply company in Warrensville Heights, Ohio, as its Chief Financial Officer (CFO). This role allowed him access to sensitive data such as payroll, expenditures, accounts payable, and company credit cards. He created fake payroll records to receive unauthorized payments, with amounts ranging from about $5,000 to $20,000 per transaction in addition to his regular salary.

In December 2023, he began his bid for a seat on the Ohio Senate representing District 28. He utilized an online fundraising platform to collect donations toward his election campaign which were deposited into a designated "Leissler For Ohio" bank account. Using his employer's company credit cards, Leissler proceeded to make unauthorized donations to his own election campaign. Then, he would request a refund of the donation.

The refund request would trigger the fundraising platform to withdraw funds from the "Leissler for Ohio" bank account. However, Leissler changed the bank account associated with his campaign to a different, non-existent bank account before the funds could be withdrawn to process the refund.

Leissler also had access to a second source of funds through a local fraternal order of police (FOP). From about December 2021 to November 2024, he was the treasurer for the organization and held a debit card and checkbook for the FOP account, which he used to make numerous unauthorized withdrawals and expenditures. He regularly reported to FOP leadership that the account balance was significantly higher than he knew it to be.

Federal investigators found that Leissler used embezzled funds to charter private planes, travel, provide a down payment for a vacation property in South Carolina, and make mortgage payments for the vacation property as well as his residential home. He also used funds to pay for credit cards, vehicles, cryptocurrency mining equipment, and to start up a side business. He also paid for advertising to encourage voters to support his election to the Ohio Senate.

Leissler's actions resulted in victims being defrauded of approximately $4.5 million in combined losses. (Source)

Finance Manger For Charity Sentenced To Prison For Embezzling $1.6 Million+ / Used Funds For Air Travel, Condo, Etc. - December 10, 2025

Carrie Grant pleaded guilty on August 11, 2025, to one count of wire fraud.

Over a period of years from November 2017 to June 2023, Grant abused her role as the finance manager of the charity, depositing charity money into her personal account while creating fraudulent records to cover her tracks. Grant spent the money on, among other things, first-class air travel, floor seats for a Golden State Warriors game, box seats for a San Francisco 49ers game, and a condominium in Hawaii. In total, Grant stole more than $1.6 million dollars from the non-profit organization. (Source)

Company Bookkeeper Of 40 Years Indicted On $205,000+ Of Wire Fraud For 5 Years / Used Funds To Make 474 Purchases On Amazon - December 22, 2025

Angela Conley worked as the bookkeeper for a Bristol, Virginia-based business (Company A) for more than 40 years. As Company A's bookkeeper, Conley was responsible for, among other duties, Company A's payroll. As such, Conley had access to bank accounts and was issued a company credit card.

Beginning in January 2020 and continuing through February 2025, Conley devised a scheme to personally enrich herself through fraud by obtaining funds that belonged to Company A. Conley is accused of using her authority as bookkeeper to send wire transfers of funds from Company A's bank account to Conley's personal Capital One credit card account, her personal checking account, and to make hundreds of purchases from Amazon. These 474 items included high heel shoes, pool covers, and earrings. All of the items were delivered via the U.S. Postal Service or commercial interstate carrier.

Conley is accused of sending 38 payments totaling $139,246 from Company A's bank account to her personal credit card account without authorization.

In addition, the indictment alleges that Conley transferred funds from Company A's bank account to Verizon, BVU Authority, and the Virginia Department of Taxation as payment for Conley's personal bills. These alleged payments were also made without authorization.

Conley is also alleged to have used her position as bookkeeper to transfer funds from Company A's bank account to her own personal bank accounts and 401K accounts. Conley altered her paycheck, causing 29 fraudulent payments to be sent from Company A's bank account to her personal bank account.

In all, between January 2020 and February 2025, Conley caused $205,889 in fraudulent transactions to be made. (Source)

EMPLOYEES' WHO EMBEZZLE / STEAL THEIR EMPLOYERS MONEY TO SUPPORT THEIR PERSONAL BUSINESS

No Incidents To Report

SHELL COMPANIES / FRAUDULENT INVOICE BILLING SCHEMES

No Incidents To Report

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

No Incidents To Report

THEFT OF ORGANIZATIONS ASSESTS
No Incidents To Report

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

EMPLOYEE DRUG & ALCOHOL RELATED INCIDENTS
Director Of Nursing For County Health Center Pleads Guilty To Stealing Fentanyl For Personal Use - December 16, 2025
On January 19, 2023, Kailyn Marie Smotherman was discovered to have been tampering with controlled substances at the Garfield County Health Center in Jordan, Montana, where she worked as the Director of Nursing.

Staff at the facility entered Smotherman's locked office to retrieve a narcotics log and noticed several suspicious items, including hospital stock narcotics, an IV pole, tourniquets, needles, IV equipment, replacement vial caps, replacement medication labels, and what appeared to be blood on many surfaces. During a subsequent search of the office, staff and law enforcement found numerous vials of fentanyl that had been tampered with (caps removed and replaced) or had been emptied. They also discovered other controlled substances that had been replaced.

Staff reported concerns patients may have received saline solution instead of pain medication in the months preceding the incident.

A forensic chemist with the Food and Drug Administration conducted an analysis of the containers confiscated from Smotherman's office and concluded the controlled substances had been tampered with and adulterated. (Source)

OTHER FORMS OF INSIDER THREATS
No Incidents To Report

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

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

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

EMPLOYEES INVOLVED IN ROBBING EMPLOYER
No Incidents To Report

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES' EMPLOYEES' INVOLVED IN TERRORISM

No Incidents To Report

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

INSIDER THREATS DEFINITION / TYPES

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 / 32 CFR Part 117 & Other Sources) and be expanded. While other organizations have definitions of Insider Threats, they can also be limited in their scope.

The information complied below was gathered from research conducted by the National Insider Threat Special Interest Group (NITSIG), and after reviewing NITSIG Monthly Insider Threat Incidents Reports.

WHO CAN BE AN INSIDER THREAT?

- ☐ Outsider With Connections To Employee (Relationship, Marriage Problem, Etc. Outsider Commits Workplace Violence, Etc.)
- ☐ Current & Former Employees / Contractors - Trusted Business Partners
- ☐ Non-Malicious / Unintentional Employees (Accidental, Carelessness, Un-Trained, Unaware Of Policies, Procedures, Data Mishandling Problems, External Web Based Threats (Phishing / Social Engineering, Etc.)
- ☐ Disgruntled Employees (Internal / External Stressors: Dissatisfied, Frustrated, Annoyed, Angry)
- ☐ Employees Transforming To Insider Threats / Job Jumpers (Taking Data With Them)
- ☐ Negligent Employees (**1** - Failure To Behave With The Level Of Care That A Reasonable Person Would Have Exercised Under The Same Circumstance) (**2** - Failure By Action, Behavior Or Response) (**3** - Knows Security Policies & Procedures, But Disregards Them. Intentions May Not Be Malicious)
- ☐ Opportunist Employees (**1** - Someone Who Focuses On Their Own Self Interests. No Regards For Impacts To Employer) (**2** - Takes Advantage Of Opportunities (Lack Of Security Controls, Vulnerabilities With Their Employer) (**3** - Driven By A Desire To Maximize Their Personal Or Financial Gain, Live Lavish Lifestyle, Supporting Gambling Problems, Etc.)
- ☐ Employees Under Extreme Pressure Who Do Whatever Is Necessary To Achieve Goals (Micro Managed, Very Competitive High Pressure Work Environment)
- ☐ Employees Who Steal / Embezzlement Money From Employer To Support Their Personal Business
- ☐ Collusion By Multiple Employees To Achieve Malicious Objectives
- ☐ Cyber Criminals / External Co-Conspirators Collusion With Employee(s) To Achieve Malicious Objectives (Offering Insiders Incentives)
- ☐ Compromised Computer – Network Access Credentials (Outsiders Become Insiders)
- ☐ Geopolitical Risks (Employee Disgruntled Because Of Country Employer Supports. Employee Divided Loyalty Or Allegiance To U.S. / Foreign Country)
- ☐ Employees Involved In Foreign Nation State Sponsored Activities (Recruited - Incentives)
- ☐ Employees Ideological Causes (Promoting Or Supporting Political Movements To Engage In Activism Or Committing Acts Of Violence In The Name Of A Cause, Or Promoting Or Supporting Terrorism)
- ☐ Geopolitical Risks (Employee Disgruntled Because Of Country Employer Supports. Employee Divided Loyalty Or Allegiance To U.S. / Foreign Country)

INSIDER THREAT DAMAGING ACTIONS CONCERNING BEHAVIORS

There are many different types of Insider Threat incidents committed by employees as referenced below. While some of these incidents may take place outside the workplace, employers may still have concerns about the type of employees they are employing.

- ☐ Facility, Data, Computer / Network, Critical Infrastructure Sabotage By Employees (Arson, Technical, Data Destruction, Etc.)
- ☐ Loss Or Theft Of Physical Assets By Employees (Electronic Devices, Etc.)
- ☐ Theft Of Data Assets By Employees (Espionage (National Security, Corporate, Research), Trade Secrets, Intellectual Property, Sensitive Business Information, Etc.)
- ☐ Unauthorized Disclosure Of Sensitive, Non-Pubic Information (By Using Artificial Intelligence Websites Such as ChatGPT, OpenAI, Etc. Without Approval
- ☐ Theft Of Personal Identifiable Information By Employee For The Purposes Of Bank / Credit Card Fraud
- ☐ Financial Theft By Employees (Theft, Stealing, Embezzlement, Wire Fraud - Deposits Into Personal Banking Account, Improper Use Of Company Charge Cards, Travel Expense Fraud, Time & Attendance Fraud, Etc.)
- ☐ Contracting Fraud By Employees (Kickbacks & Bribes That Can Have Damaging Impacts To Employer)
- ☐ Money Laundering By Employees
- ☐ Fraudulent Invoices And Shell Company Schemes By Employees
- ☐ Employee Creating Hostile Work Environment (Unwelcome Employee Behavior That Undermines Another Employees Ability To Perform Their Job Effectively)
- ☐ Workplace Violence Internal By Employees (Arson, Bomb Threats, Bullying, Assault & Battery, Sexual Assaults, Shootings, Deaths, Etc.)
- ☐ Workplace Violence External (Threats From Outside Individuals Because Of Relationship, Marriage Problems, Etc.) Directed At Employee(s))
- ☐ Employees' Working Remotely Holding 2 Jobs In Violation Of Company Policy
- ☐ Employees Involved In Drug Distribution
- ☐ Employees Involved In Human Smuggling, The Possession / Creation Of Child Pornography, The Sexual Exploitation Of Children

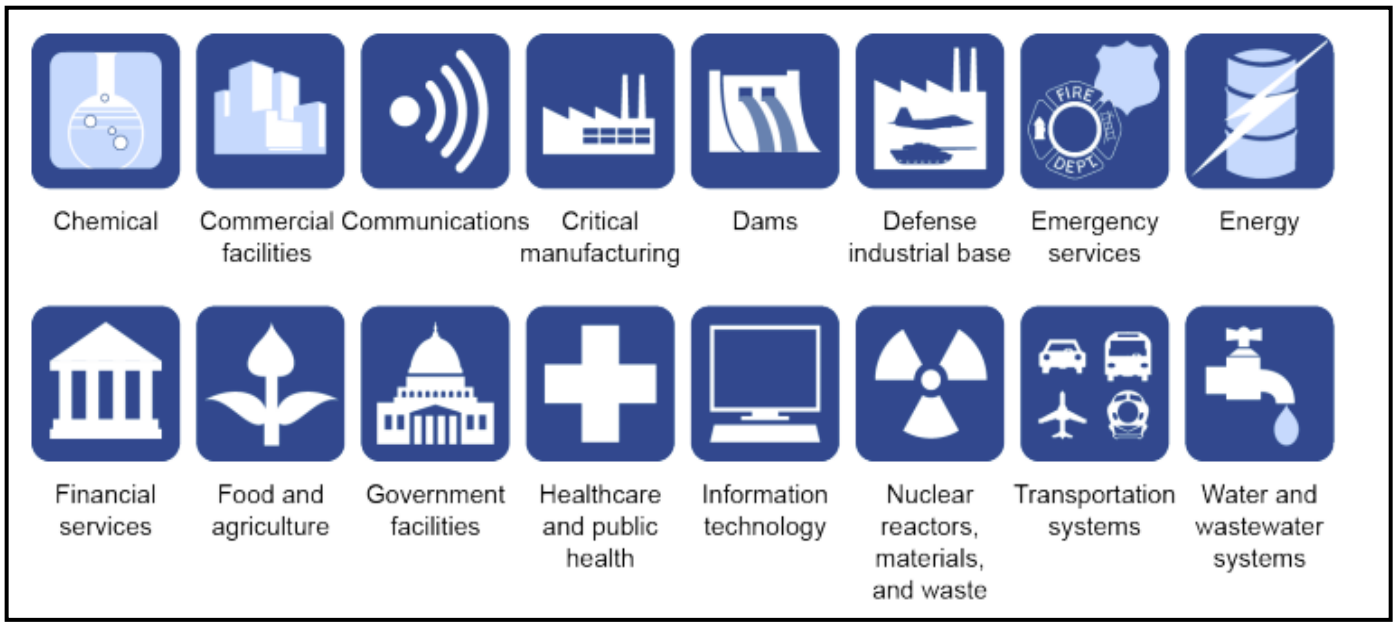
Other Damaging Impacts To An Employer From An Insider Threat Incident

- ☐ Stock Price Reduction
- ☐ Public Relations Expenditures
- ☐ Customer Relationship Loss, Devaluation Of Trade Names, Loss As A Leader In The Marketplace
- ☐ Compliance Fines, Data Breach Notification Costs
- ☐ Increased Insurance Costs
- ☐ Attorney Fees / Lawsuits
- ☐ Increased Distrust / Erosion Of Morale By Employees, Additional Turnover
- ☐ Employees Lose Jobs, Company Downsizing, Company Goes Out Of Business

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

NITSIG monthly Insider Threat Incidents Reports reveal that governments, businesses and organizations of all types and sizes are not immune to the Insider Threat problem.

- ☐ 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
- ☐ Schools, Universities, Research Institutes
- ☐ Non-Profits Organizations, Churches, etc.
- ☐ Labor Unions (Union Presidents / Officials, Etc.)
- ☐ And Others



WHAT CAN MOTIVATE EMPLOYEES TO BECOME INSIDER THREATS?

EMPLOYER – EMPLOYEE TRUST RELATIONSHIP BREAKDOWN

An employer - employee relationship can be described as a circle of trust / 2 way street.

The employee trusts the employer to treat them fairly and compensate them for their work.

The employer trusts the employee to perform their job responsibilities to maintain and advance the business.

When an employee feels **This Trust Is Breached**, an employee may commit a **Malicious** or other **Damaging** action against an organization

Cultivating a culture of trust is likely to be the single most valuable management step in safeguarding an organization's assets.

After new employees have been satisfactorily screened, continue the trust-building process through on-boarding, by equipping them with the knowledge, skills and appreciation required of trusted insiders.

Listed below are some of the common reasons that trusted employees develop into Insider Threats.

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

TD Bank Pleads Guilty To Money Laundering Conspiracy / Employees Accepted $57,000+ In Bribes / 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+ / GS Agrees To Pay $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)

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 Fraudulent 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)

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)

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)

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)

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)

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)

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)

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)

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)

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)

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 daily and monthly with the latest incidents.
There is NO REGISTRATION required to download the reports.

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 (**6,700+ 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 POSTINGS ON TWITTER / X

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

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present
http://www.insiderthreatincidents.com **or**
https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

SPECIALIZED REPORTS

Produced By:
National Insider Threat Special Interest Group (NITSIG)
Insider Threat Defense Group (ITDG)

Employee Personal Enrichment Using Employers Money / November 2025

You might be amazed at the many reasons employees steal money from their employers.

Many employees justify stealing money from their employers for a variety of reasons, often stemming from a combination of variables that can include, but are not limited to; being overworked, underpaid, job dissatisfaction, lack of promotion, financial pressure, perceived injustices, etc. Perceived injustices in the workplace can lead to disgruntled employees. These employees may feel wronged by their employer and seek to "even the score" through financial theft. Employees may feel the company owes them.

Employees may simply be driven by a desire to maximize their financial assets, live a lavish lifestyle, support their personal business, need funds to pay for child support, home improvements or pay medical bills, or need money to support their gambling problems, etc.)

This report provides indisputable proof that a malicious employee can be anyone in any type of organization or business, from a regular worker to senior management and executives.

This report covers the year 2025 and provides an in-depth snapshot of what employees do with the money they steal from their employers. Download Report

Insider Threat Fraudulent Invoices & Shell Schemes Report / August 2025

Pages 6 to 24 of this report will highlight employees that are involved in **1)** Creating fraudulent invoices (For Products, Services And Vendors That Don't Exist) **2)** Manipulating legitimate invoices **3)** Working with external co-conspirators / vendors to create fraudulent or manipulated invoices.

These fraudulent invoices will then be submitted to the employer for payments to a shell company created by the employee, who will receive payment to a shell company bank account or through other methods. These fraudulent invoices schemes may happen just once or become reoccurring.

Employees may also collaborate with other employees, vendors or third parties to approve fraudulent invoices in exchange for kickbacks. An accounts payable employee might work with a vendor to create fraudulent invoices, and then the employee ensures the invoices are approved. Then the employee and vendor share the proceeds after the payment is issued.

These schemes can be disguised as legitimate business transactions, making them difficult to detect without proper internal controls. A shell company often consists of little more than a post office box and a bank account.

These schemes are often perpetrated by an opportunist employee, whose primarily focuses is for their own self-interest. They take advantage of opportunities (Lack Of Controls, Vulnerabilities) within an organization, often with little regard for the ethics, consequences or impacts to their employers. They are driven by a desire to maximize their personal financial gain.

From small companies to Fortune 500 companies, this report will provide a snapshot of fraudulent invoicing and shell companies schemes that are quite common.

This report and other monthly reports produced by the NITSIG provide clear and indisputable evidence that Insider Threats is not just as a data security, employee monitoring, technical, cyber security, counterintelligence or investigations problem

Why Insider Threats Remain An Unresolved Cybersecurity Challenge

Produced By: IntroSecurity: NITSIG - ITDG / June 2025

The report was developed in collaboration with IntroSecurity and the NITSIG. It provides a practical and real world approach to Insider Risk Management (IRM), based off of research of actual Insider Threat incidents and the maturity levels of IRM Programs (IRMP's)

This report provides detailed recommendations for mitigating Insider Risks and Threats. It outlines strategies for strengthening IRMP's and cross-departmental governance, adopting advanced detection techniques, and fostering key stakeholder and employee engagement to protect an organizations Facilities, Physical Assets, Financial Assets, Employees, Data, Computer Systems - Networks from the risky or malicious actions of employees.

The goal of this report is to provide anyone involved in managing or supporting an IRM Program with a common sense approach for identifying, deterring, mitigating and preventing Insider Risk and Threats. Through research, collaboration and conversations with NITSIG Members, and discussions with organizations that have experienced actual Insider Threat incidents, the report outlines recommendations for an organization to defend itself from the very costly and damaging Insider Threat problem. (Download Report)

U.S. Government Insider Threat Incidents Report For 2020 To 2024
The NITSIG was contacted by Senator Joni Ernst's office in December 2024, and a request was made to write a report about Insider Threats in the U.S. Government for the Department Of Government Efficiency (DOGE). (Download Report)

Department Of Defense (DoD) Insider Threat Incidents Report For 2024
The traditional norm or mindset that DoD employees just steal classified information or other sensitive information is no longer the case. There continues to be an increase within the DoD of financial fraud, contracting fraud, bribery, kickbacks, theft of DoD physical assets, etc. (Download Report)

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. (Download Report)

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

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

Jim Henderson, CISSP, CCISO
Founder / Chairman Of The National Insider Threat Special Interest Group
Founder / Director Of Insider Threat Symposium & Expo
Insider Threat Researcher / Speaker
FBI InfraGard Member
561-809-6800
jimhenderson@nationalinsiderthreatsig.org
www.nationalinsiderthreatsig.org

INSIDER THREAT DEFENSE GROUP

INSIDER RISK MANAGEMENT PROGRAM EXPERTS
TRAINING & CONSULTING SERVICES

The Insider Threat Defense Group (ITDG) provides organizations with the **core skills / advanced knowledge, resources and technical solutions** to identify, manage, prevent and mitigate Insider Risks - Threats.

Since 2009, the ITDG has had a long standing reputation of providing our clients with proven experience, past performance and exceptional satisfaction. ITDG training courses and consulting services have empowered organizations with the knowledge and resources to develop, implement, manage, evaluate and optimize a comprehensive Insider Risk Management (IRM) Program (IRMP) for their organizations.

Being a pioneer in understanding Insider Risks - Threats from both a holistic, non-technical and technical perspective, the ITDG stands at the forefront of helping organizations safeguard their assets (Facilities, Employees, Financial Assets, Data, Computer Systems - Networks) from one of today's most damaging threats, the Insider Threat. **The financial damages from a malicious or opportunist employee can be severe, from the MILLIONS to BILLIONS.**

With 15+ years of IRMP expertise, the ITDG has a deep understanding of the collaboration components and responsibilities required by key stakeholders, and the many underlying and interconnected cross departmental components that are critical for a comprehensive IRMP. This will ensure key stakeholders are **universally aligned** with the IRMP from an enterprise / holistic perspective to address the Insider Risk - Threat problem.

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 Evaluation & Optimization Training Course (Develop, Management, Enhance)
- ✓ Insider Threat Investigations & Analysis Training Course With Legal Guidance From Attorney
- ✓ 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

STUDENT / CLIENT SATISFACTION

ITDG training courses have been taught to over **1000+** individuals. Our clients have endorsed our training and consulting services as the most affordable, next generation and value packed training for IRM.

Even our most experienced students that have attend our training courses, or taken other IRM Program training courses and paid substantially more, state that they are amazed at the depth of the training content and the resources provided, and are very satisfied they took the training and learned some new concepts and techniques for IRM.

Our client satisfaction levels are in the **EXCEPTIONA**L range, due to the fact that the ITDG approaches IRM from a real world, practical, strategic, operational and tactical perspective. You are encouraged to read the feedback from our clients on this link.

The ITDG Has Provided IRM Program Training / Consulting Services To An Impressive List Of 700+ 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, 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 Risk Management Program Training Course Instructor / Consultant
Insider Threat Investigations & Analysis Training Course Instructor / Analyst
Insider Risk / Threat Vulnerability Assessor
561-809-6800
jimhenderson@insiderthreatdefensegroup.com
www.insiderthreatdefensegroup.com
LinkedIn ITDG Company Profile
Follow Us On Twitter / X: @InsiderThreatDG