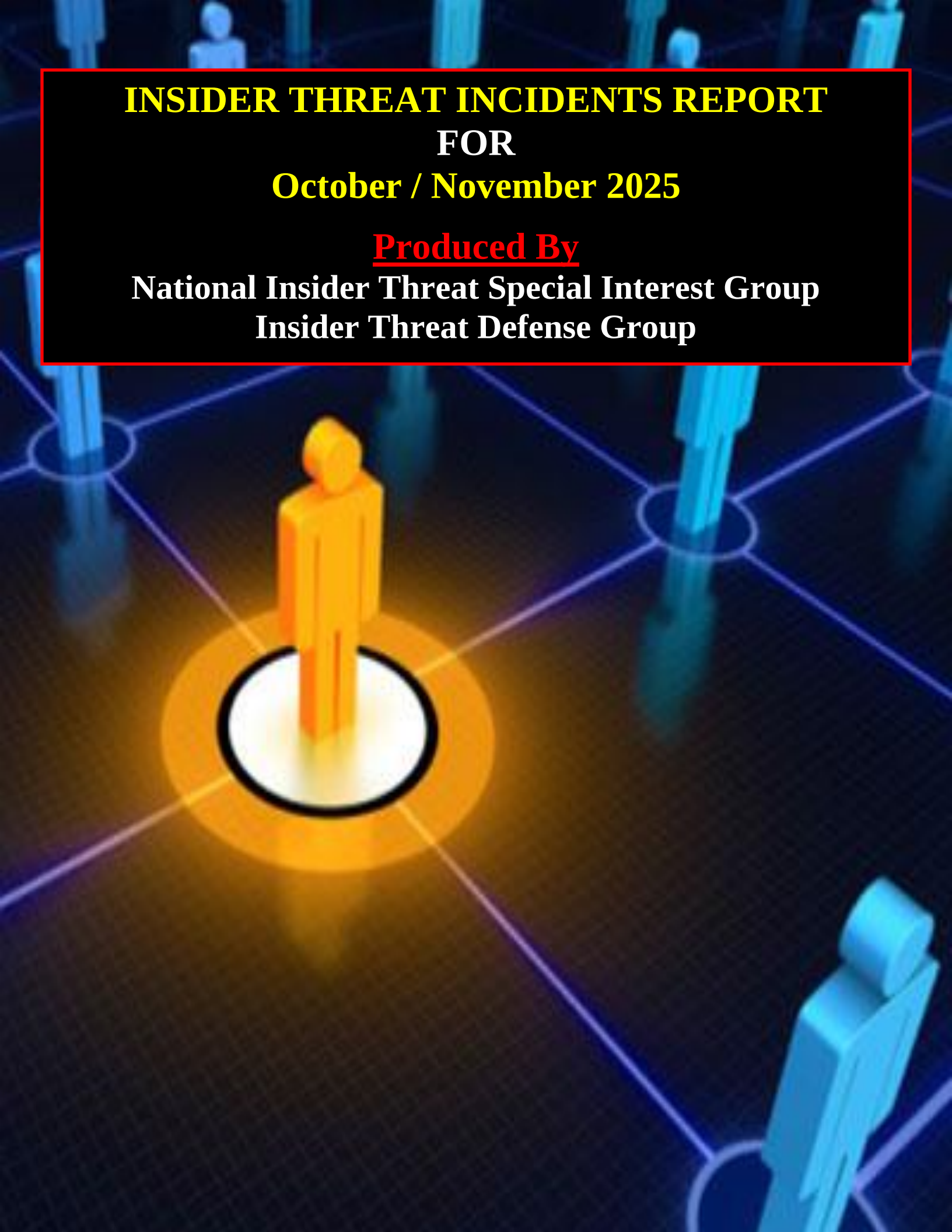


INSIDER THREAT INCIDENTS REPORT

FOR

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

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

Taking a **PROACTIVE** rather than **REACTIVE** approach is critical to protecting an organization from employee risks / threats, especially when the damages from employees' can be into the **MILLIONS** and **BILLIONS**, as this report and other shows. **Companies have also had large layoffs or gone out of business because of the malicious actions of employees.**

These monthly reports are recognized and used by Insider Risk Program Managers and security professionals working for major corporations, as an educational tool to gain support from CEO's, C-Suite, key stakeholders and supervisors for Insider Risk Management (IRM) Program's. The incidents listed on pages **4 to 32** 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 OCTOBER / NOVEMBER 2025

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS
No Incidents To Report

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 - October 28, 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.

That marathon of research formed the foundation for Robinson's upcoming Black Hat Europe briefing, "Understanding Trends & Patterns in Insider Threat: Analysis of 1,000+ Cases." He plans to reveal what he calls "the uncomfortable truths" about insider threats — truths that challenge many long-held assumptions about who the bad actors are, when they strike, and how they operate.

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 The Malicious Insiders?
One-quarter of the malicious insiders were top executives.

"These were senior people — vice presidents, presidents — 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

U.S. State Department Employee Arrested For Removing 1000+ Top Secret Classified Documents And Storing At Home - October 14, 2025

Ashley Tellis held a Top Secret security clearance with Sensitive Compartmented Information (SCI) access. He has worked for the U.S. Department of State since 2001 and currently serves in addition as a contractor for the Department of Defense's Office of Net Assessment. He also serves as a Senior Fellow at the Carnegie Endowment for International Peace.

As alleged, Tellis accessed classified documents on multiple occasions from secured facilities, including a Sensitive Compartmented Information Facility (SCIF) at the Department of Defense and a secure computer system at the Department of State. In one instance, Tellis altered the filename of a classified document, printed portions of it under the altered title, and then deleted the re-named file. In another incident, he was observed placing classified materials into a notepad and concealing them within his personal briefcase before leaving a secured government facility.

During a court-authorized search of Tellis's residence, investigators recovered over 1,000 pages of documents with classification markings, including materials labeled SECRET and/or TOP SECRET. These documents were found in locked filing cabinets, in a basement home office, and in trash bags stored in a basement utility area. (Source)

U.S. Postal Service Employee Pleads Guilty To Stealing $4,000 In Treasury Checks And Committing PPP Load Fraud / Used Funds For Clothing & Other Personal Items - November 5, 2025

In 2023, Vershun Weaver worked as a mail carrier with the U.S. Postal Service.

In July 2023, a postal employee who borrowed Weaver's mail delivery truck found Weaver's wallet and turned it in to a supervisor. The supervisor looked inside the wallet for identification and saw two U.S. Treasury checks addressed to customers on Weaver's delivery route. One check was for approximately $2,500, and the other was for $1,500.

During a subsequent investigation, federal agents located in Weaver's personal vehicle several additional pieces of mail addressed to other victims on Weaver's delivery route. Agents also discovered that Weaver had fraudulently obtained a PPP loan. To support his application for the loan, Weaver submitted a fake income tax document that he knew had not been filed with the Internal Revenue Service. Weaver spent the proceeds of his PPP fraud on clothes and other personal items that were prohibited under the terms of the pandemic relief loan. (Source)

Florida Congresswoman Indicted For Stealing $5 Million Of FEMA Relief Funds For Campaign Use - November 19, 2025

A Miami grand jury indicted Rep. Sheila McCormick, D-Fla., on charges of allegedly stealing millions of dollars in disaster relief funds to make illegal campaign contributions, the Department of Justice stated.

The Florida Democrat allegedly conspired to steal $5 million in Federal Emergency Management Agency (FEMA) funds alongside her brother Edwin Cherfilus and numerous co-defendants.

Prosecutors alleged that the defendants routed the funds through multiple accounts to disguise their source and that a significant portion of the misappropriated funds were used as candidate contributions to McCormick's 2021 congressional campaign or for their personal benefit.

Both McCormick and her brother worked through their family healthcare company on a FEMA-funded COVID-19 vaccination staffing contract in 2021, according to the indictment. The company received an overpayment of $5 million in FEMA funds in July 2021, prosecutors alleged. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Human Resources Manager Pleads Guilty To Engaging In Practice Of Hiring Illegal Aliens To Work For Military Bases & Ports - November 26, 2025

San Diego Powder & Protective Coatings and the company's hiring manager, Karli Buxton, pleaded guilty to engaging in a practice of hiring undocumented immigrants without authorization to work in the United States.

The company, a government contractor, also agreed to forfeit $230,000 that it gained from engaging in the practice.

Since 2023, Buxton was responsible for verifying that new employees were eligible to work in the United States. As part of her plea agreement, she admitted that she was aware certain employees were presenting fraudulent documents to show their authorization to work in the United States, but she accepted the documents and hired them for employment at the company.

The company further admitted that it had frequently sent employees to work in secure locations such as military bases or ports of entry and avoided sending any employees working illegally to these secure locations where they would be subject to further screening. The company also admitted the aliens it employed in its warehouses often had access to military equipment such as components for submarines or aquatic vehicles used by the United States Navy. (Source)

Army Colonel (Now Retired) Pleads Guilty To Unauthorized Communication Of Classified Military Strike Plans To Woman He Met Online - November 14, 2025

In October 2024, Kevin Luke was a government civilian employee at United States Central Command in Tampa, Florida.

Luke met a woman online and began communicating with her via his personal cellphone and computer. On October 1, 2024, Luke sent that woman a text message stating, "sent to my boss earlier, gives you a peak at what I do for a living." Luke then sent a photograph of a computer screen displaying a classified email message that he had authored and sent using a government email address intended for classified email communications. The email contained classified markings of SECRET//REL TO USA, FVEY that Luke had himself added.

The photograph of the classified email that Luke sent to the woman discussed a then-future U.S. military operation. This information was classified at the time and remains classified. The photograph of the classified email also revealed the number of targets of the planned U.S. military operation as well as the future date of the operation, the means of executing the operation, and the goal of the operation. Luke knew that his personal cellphone was not authorized for storing or transmitting national defense information, and that the woman was not authorized to receive national defense information. (Source)

U.S. Army Sergeant Sentenced To Prison For Delivering Classified Information To China - October 30, 2025

Joseph Schmidt was an active-duty soldier from January 2015 to January 2020. His primary assignment was at Joint Base Lewis-McChord (JBLM) in the 109th Military Intelligence Battalion. In his role, Schmidt had access to SECRET and TOP SECRET information.

After his separation from the military, Schmidt reached out to the Chinese Consulate in Turkey and later, the Chinese security services via email offering national defense information.

In March 2020, Schmidt traveled to Hong Kong and continued his efforts to provide Chinese intelligence with classified information he obtained from his military service. He created multiple lengthy documents describing various "high level secrets" he was offering to the Chinese government.

He retained a device that allows for access to secure military computer networks and offered the device to Chinese authorities to assist them in efforts to gain access to such networks. Just 17 days after he made the approach to the Chinese intelligence contacts, he was granted a long sought-after work visa for China.

Schmidt remained in China, primarily Hong Kong, until October 2023, when he flew to San Francisco. He was arrested at the airport. (Source)

Department Of Veterans Affairs Employee Charged With Helping Veterans Receive Millions In Fraudulent Disability Payments And Taking Kickbacks - November 14, 2025

Until June of 2025, Rikkels was employed by the Department of Veterans Affairs and was responsible for reviewing and approving VA disability claims from veterans. During this time-period he negotiated with veterans for assistance in their VA claims and demanded payment from them, all while he was taking official action on their claims in violation of government ethics laws.

Through these false claims, the veterans fraudulently obtained millions of dollars in VA disability payments and backpay, and Rikkels received millions of dollars in payments from the veterans in return for his work on their behalf.

The indictment also alleges that Rikkels frequently requested that veterans who lived in the local area meet him to make payments in cash to minimize what he would have to pay in taxes. According to court records, the investigation revealed that during just a three-month period between February and May of 2025, Rikkels met with at least four local veterans and received a total of $57,000 in cash payments from them. On November 13, 2025, agents searched Rikkels, his vehicle, and residence and seized a total of over $280,000 in cash. (Source)

U.S. Navy Employee Arrested For Active Shooter Hoax' At N.J.'s Joint Base McGuire-Dix-Lakehurst Because She Was Ostracized By Her Co-Workers - October 1, 2025

A federal employee is in custody for allegedly staging an "active shooter hoax" that prompted a lockdown Tuesday morning at New Jersey's Joint Base McGuire-Dix-Lakehurst, one of the nation's largest military bases.

Acting U.S. Attorney Alina Habba posted on X on Tuesday night that "false information" had been provided to the base by a civilian employee of the federal government. In a criminal complaint filed in federal court, the suspect in custody was later identified as Malika Brittingham, a U.S. Navy employee assigned to work at the base.

Charging documents say Brittingham sent a text message to an unnamed person around 10:15 a.m. warning of an active shooter, CBS News reported. Brittingham claimed to have heard five or six shots fired and said she was hiding in a closet with her co-workers, prosecutors allege. The recipient of the text message then notified the base's operation center and called 911, leading to the lockdown and an emergency response at the facility.

Brittingham allegedly admitted to investigators that she sent the text message because she had been "ostracized by her co-workers" at the base and hoped fabricating an active shooter situation "would allow them to 'trauma bond'" over the experience. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

14 Law Enforcement Officials Arrest In Mississippi Drug Conspiracy Takedown By FBI - October 30, 2025

20 Mississippi and Tennessee individuals were arrested today on criminal charges related to their alleged participation in a drug trafficking conspiracy in the Mississippi delta.

According to court documents, Brandon Addison, Javery Howard, Milton Gaston, Truron Grayson, Bruce Williams, Sean Williams, Dexture Franklin, Wendell Johnson, Marcus Nolan, Aasahn Roach, Jeremy Sallis,

Torio Chaz Wiseman, Pierre Lakes, Derrik Wallace, Marquivious Bankhead, Chaka Gaines, Martavis Moore, Jamario Sanford, Marvin Flowers, and Dequarian Smith are all charged with drug distribution. These individuals were arrested in numerous counties within the Northern District of Mississippi and Shelby County, TN.

In addition, 19 individuals are charged with violating federal firearm laws pertaining to carrying a firearm in relation to a drug trafficking crime. As stated in the indictments, 14 of these individuals were local law enforcement officials in the Mississippi delta. (Source)

County Sheriff, 2 Employees Plead Guilty For Fraudulent Use Of $200,000 Of Public Funds - October 30, 2025

The Spartanburg County Sheriff's Office Chaplain's Benevolence Fund (South Carolina) is a non-profit organization that provides financial and emotional assistance to officers of the Spartanburg County Sheriff's Office during times of need, such as bereavement, financial difficulties, and traumatic line-of-duty events.

Charles Wright, in his capacity as sheriff, hired Amos Durham as the Director of the Benevolence Fund. In that position, Durham was responsible for administering the fund. Durham and Wright abused their positions and conspired to siphon public funds from the Benevolence Fund for their private use.

In March 2005, Wright hired Lawson Watson as an employee of the Spartanburg County Sheriff's Office. From at least as early as January 2021 through March 2025, Watson certified on his timesheet that he worked a full-time job. In fact, Watson received a full salary and benefits for work that he did not perform. Wright allowed Watson to continue to fraudulently receive a paycheck and benefits of approximately $200,000 for work that he did not perform.

In May of 2023 through September 2023, Wright knowingly and intentionally obtained 147 pills of oxycodone and hydrocodone by misrepresentation from an individual after representing that the pills would be turned in and destroyed as part of the "take back" narcotic disposal program administered by the Spartanburg County Sheriff's Office. In fact, Wright was obtaining the narcotics for his own personal use. (Source)

Deputy Sheriff Pleads Guilty To $145,000 Of Bank Fraud - November 18, 2025

In December 2018 and January 2019, while employed as a Deputy Sheriff Officer with the City of Philadelphia, Darryl Wells submitted eight fraudulent loan and credit applications to financial institutions in which he falsely and materially overstated his monthly income and, in some instances, attached forged paystubs.

In total, Wells received $145,000 in fraudulently obtained proceeds, which he immediately spent or transferred, and the financial institutions were not repaid. (Source)

County Corrections Officer Pleads Guilty To $54,000+ COVID Unemployment And Loan Fraud Scheme - November 25, 2025

Christne Orisca was a Corrections Officer with the Suffolk County Sherriff's Department in Massachusetts.

From late 2021 to December 2024. Orisca fraudulently applied for pandemic unemployment and small business loan benefits while working full-time, initially for a security company and later for a delivery company. While employed full-time, Orisca collected approximately $54,700 in unemployment benefits and small business loan funds. (Source)

Federal Correctional Officer Charged For Accepting $43,000 In Bribes To Smuggle Contraband Into Prison - November 14, 2025

Karen Torres was a public official employed by the United States Department of Justice, Federal Bureau of Prisons, as a correctional officer. She worked at the Coleman Federal Correctional Complex (FCC Coleman) in Sumter County. Between May 2022 and March 3, 2025.

Torres received $43,550 in monetary payments in return for being influenced to smuggle contraband into the prison. (Source)

County Jail Employee Accused Of Stealing $27,000 From Inmates To Help With Her Financial Problems - October 1, 2025

A former jail employee turned herself in after an investigation learned she'd stolen over $27,000 from inmate accounts. Haley Atherton, 26, worked as a booking specialist at the Elkhart County Jail starting in June 2023, and has since been terminated.

The investigation revealted that from July 2024 to June 2025, Atherton used 600 debit cards containing skimmed funds from several former inmates' Trust Funds.

Security camera footage recorded Atherton making these cards and slipping them in her pockets or between pages of her notebook. The affidavit says she was also seen on camera using the cards in various stores, including a Meijer and a smoke shop.

Detectives spoke with Atherton on June 18, where she admitted to skimming inmate funds to help with her financial issues.

She explained to investigators that no one taught her how to take from the Trust Funds, and she "didn't think anyone would care" but "knew they would care, (justifying) it because she didn't want to starve or lose this or that. Atherton said she'd use the money to buy dinner or put toward a new car.

Court documents say Atherton was surprised learning she made over 600 Trust Fund debit cards, but showed remorse. "(She) advised that there is not much she can do now but take it on the chin and deal with what comes from this," police said. In total, Atherton stole $27,239.49 from former inmate accounts. (Source)

U.S. Border Patrol Agent Sentenced To Prison For Accepting $20,000 In Bribes - November 17, 2025
Jorge Jimenez was employed as a United States Border Patrol Agent since 2010.

Between June 2024 and early October 2024, Jimenez was assigned to the I-19 Checkpoint, and conspired with at least two individuals located in Mexico, to allow previously agreed-upon "load" vehicles to pass through his designated checkpoint lane without inspection.

The individuals in Mexico handled arrangements and the receipt of payment, and Jimenez allowed the vehicles to pass through his assigned lane and provided information about ctivities at the checkpoint to his coordinators. Jimenez expected to be paid approximately $20,000, with the money exchanged in Mexico. (Source)

Minnesota Police Department Employee Charged In Major Narcotics Trafficking Investigation - October 14, 2025
The St. Paul Police Department in Minnesota confirmed the arrest of one of its now-former employees in connection to a "major narcotics trafficking investigation."

The Washington County Sheriff's Office said an arrest was made with the county drug task force seizing 10 lbs of methamphetamine, nearly 2 lbs of fentanyl, 10 g of cocaine and two handguns.

St. Paul police said the suspect, a community engagement specialist for the department, is facing criminal charges and "has since been terminated." (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS
70 Employees Of New York City Housing Authority Convicted For Accepting $2.1 Million+ In Bribes For $15 Million+ Worth Of Contracts - November 25, 2025
The employees, all of whom were New York City Housing Authority (NYCHA) 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 employees were collectively responsible for accepting over $2.1 million in bribes in exchange for awarding NYCHA contracts worth over $15 million. As a result of the convictions, the defendants will collectively pay over $2.1 million in restitution to NYCHA and will forfeit over $2 million in criminal proceeds.

The employee 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.

NYCHA is the largest public housing authority in the country, providing housing to 1 in 17 New Yorkers in 335 developments across the City and receiving over $1.5 billion in federal funding from the U.S. Department of Housing and Urban Development every year.

When repairs or construction work require the use of outside contractors, services must typically be purchased via a bidding process. However, at all times relevant to the cases referenced above, when the value of a contract was under a certain threshold (up to $10,000), designated staff at NYCHA developments could hire a contractor of their choosing without soliciting multiple bids. This "no-bid" process was faster than the general NYCHA procurement process, and selection of the contractor required approval of only the designated staff at the development where the work was to be performed. (Source)

Louisiana Department Of Health Employee Arrested For $22,000+ Of Medicaid Benefits Fraud - October 14, 2025

A former Louisiana Department of Health (LDH) employee (Courtney Higgins) has been arrested for filing false public records and government benefits fraud, according to Louisiana Attorney General Liz Murrill.

Murrill's office said they received a tip that Higgins had knowingly assisted a family member in concealing their income and marital status to get Medicaid benefits. It was determined that Higgins submitted a false employment verification letter to LDH for the family member.

According to Murrill's office, Higgins was aware that the family member was not eligible for Medicaid and her actions defrauded the program of about $22,536.56. (Source)

Building And Zoning Department Employee Arrested For $4,500+ Bribery And Extortion Scheme - October 2, 2025

A city of Hollywood employee in the building and zoning department has been arrested following an investigation into bribery and extortion, city officials said. Roberto Meneses, 38, was arrested on charges of unlawful compensation, bribery of a public servant, scheme to defraud, and grand theft, Broward jail records showed.

The investigation into Meneses, a zoning plans reviewer and inspector, began in May amid allegations of bribery and extortion being committed in his capacity as a city employee.

Meneses solicited money from people who needed help with permitting issues. In one instance, Meneses said he could assist a victim with a fire permit code error for $300, the affidavit said. The victim said they sent $480 to Menses through Zelle for the fire permit issue and to deal with an HOA issue, the affidavit said.

Investigators found Zelle records that showed multiple payments made to Menses for what appeared to be permit-related services from other possible victims.

Another person said she paid Meneses $500 to take care of a permitting issue, and another person paid him over $1,000 to resolve another permit issue.

Detectives found Meneses used his official position to victimize numerous homeowners, contractors and permit runner for personal monetary gain, for a total of over $4,500, the affidavit said. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

Former County Schools Maintenance Employee Sentenced To Prison For $3.4+ Million Fraud Scheme / Used Funds To Purchase Vehicles - November 20, 2025

From about November 2019 through December 2023, Michael Barker ordered custodial and janitorial supplies for Boone County Schools from Jesse Marks and his company, Rush Enterprises. These supplies included hand soap, trash can liners, face masks, face shields, and hand sanitizer.

Barker admitted that he and Marks agreed that Rush Enterprises would overbill the Boone County Board of Education for these supplies. As part of this scheme, Barker approved invoices on behalf of Rush Enterprises that significantly inflated the number of products that were actually delivered to Boone County Schools. Barker submitted these fraudulent invoices to the Boone County Board of Education, which relied on them to mail checks to Rush Enterprises using the United States Mail.

Marks deposited the checks from Boone County Schools into the business bank account for Rush Enterprises, wrote himself checks on that account that he cashed at various banks, and personally delivered some of that cash to Barker in manila envelopes. Barker admitted that he spent the cash delivered by Marks to buy vehicles and equipment and make substantial improvements to his residence.

Marks deducted the cost of the products actually delivered to Boone County Schools from the proceeds of the overbilling scheme. Boone County Schools paid Rush Enterprises $4,310,714.82 from in or about November 2019 through in or about December 2023. Barker admitted that approximately 80 percent of the total payments received by Rush Enterprises, or $3,448,571.85, was based on fraudulent invoices. (Source)

Director Of Operations & Maintenance For Boston Public Schools Charged With Receiving $870,000+ In Bribes For 11 Years - November 14, 2025

The former Director of Fleet and Facilities for the company that manages the operations and maintenance of Boston Public Schools' (BPS) fleet of school buses was arrested and charged today for allegedly soliciting bribes from vendors who worked on the buses and in the bus yards. One of the vendors who allegedly paid bribes was also arrested and charged.

Michael Muller, 59, and John Colantuoni, 60, were charged in a 21-count indictment. Muller is charged with five counts of soliciting and accepting bribes as an agent of BPS, five counts of conspiring to commit bribery, five counts of conspiring to commit honest services mail fraud and four counts of extortion. Colantuoni is charged with one count of paying bribes to Muller as an agent of BPS, one count of conspiring to commit bribery, one count of conspiring to commit honest services mail fraud and one count of obstruction of justice.

Muller's employer, the "Transportation Company," had a contract with BPS to manage the operations and maintenance of BPS' fleet of over 700 school buses. When not on the road, the buses were kept in bus yards owned by the City of Boston. Muller allegedly supervised all the Transportation Company employees who worked in the yards. According to the BPS contract, Muller's job was to "ensure that BPS's fleet is safe, well-maintained and ready for service on a daily basis."

The Transportation Company subcontracted out much of its work on the BPS contract, including to vendors who cleaned the buses, made autobody and mechanical repairs, and plowed the snow from the bus yards. Muller allegedly managed and supervised all the vendors and had the authority to fire them. The vendors gave their invoices to the Transportation Company, which forwarded them to BPS without any markup. BPS paid the invoice amounts to the Transportation Company, allegedly from its annual transportation budget funded by taxpayer money. The Transportation Company then mailed checks to the vendors.

Between 2010 and December 2021, Muller allegedly solicited and accepted a total of more than $870,000 in bribes and kickbacks from five vendors, including Colantuoni. The alleged bribes included, among other things, cash, checks, a used pickup truck worth $15,000 and $85,000 in building materials for Muller's vacation house. Muller also allegedly required one vendor to hire his adult child. (Source)

University Employee Arrested For Stealing & Selling $215,000 Worth Of Electrical Components - October 9, 2025

An East Carolina University (ECU) employee is facing charges after police say he stole more than $200,000 worth of items from the school and listed them for sale online. 39-year-old Matthew Dickson was arrested by ECU campus police. Dickson, who works as a Facilities Life Safety Technician, stole electrical components like breakers, fuses, a computer and relays in January 2023.

Warrants say he had also stolen HVAC parts valued at $78,000, video board parts, and four audio mixer monitors. In total, Dickson is accused of stealing approximately $215,000 worth of equipment from ECU, according to police.

ECU police confirmed that Dickson was also found to be listing and selling the stolen items on eBay. Police say they recovered most of the stolen property during an investigation. Dickson was charged with larceny by an employee and three counts of felony larceny. (Source)

School District Accountant Sentenced To Prison For Embezzling $92,000+ / Used Funds For His & Wifes Personal Expenses - November 25, 20257

Anthony Moon, 44, worked as the district accountant for the Savannah R-III School District (District) in Missouri.

Beginning in or about January 2023, and continuing through on or about Nov. 21, 2023, Moon embezzled funds from the District. Moon used his position at the District to write unauthorized checks to himself and his business from the District's checking account. Moon also used the District's checking account to make Automated Clearing House payments, to his and his wife's personal credit card accounts.

Moon used those embezzled funds to pay for his and his wife's personal expenses, including, among other things, Kansas City Chiefs tickets, food, travel, gas, and entertainment. The court ordered Moon to pay restitution of $92,746.99. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

IT Employee Arrested For Selling Login Credentials To Hackers Who Stole $100 Million From PIX Banking Payment Systems - July 7, 2025

Police in Brazil have arrested an employee of a prominent software company after more than $100 million was stolen through an instant payment system called PIX.

João Roque, an employee of C&M Software, was arrested by police and told them he sold his login credentials to hackers who had approached him earlier this year. Roque worked on the company's information technology team and helped the hackers breach PIX, which links Brazil's Central Bank to the country's financial institutions.

Roque sold his account and password to the hackers for about $2,700 in two separate cash payments. He allegedly told investigators that he was approached at a bar by the hackers who asked for his account details.

They later walked him through what he needed to do, which included creating separate accounts in the system and enabling remote access.

Police told the Associated Press the hackers stole more than 540 million Brazilian reais (more than $98.3 million) from at least one financial institution but likely took more from other banks and lenders. TV Globo said at least six financial institutions were impacted.

The Central Bank has shut off access to parts of C&M Software's system and police are now searching for the hackers behind the incident, identifying at least four culprits. Another 270 million reais (about $49 million) connected to the incident has been frozen by authorities. (Source)

Bank Of America Employee Sentenced To Prison For Role In $25 Million International Money Laundering & Drug Trafficking Conspiracy - November 14, 2025

In May 2023, a federal grand jury in Boston returned a superseding indictment charging 12 individuals from Massachusetts, Rhode Island, New York and California for their alleged involvement in a sophisticated international money laundering and drug trafficking organization. The network was identified in the greater Boston area in 2021 along with the leader of the organization, Jin Hua Zhang, based in Staten Island, New York, and a number of his criminal associates.

The investigation revealed that, for a fee, Zhang laundered bulk cash for drug dealers and laundered profits from other illegal businesses. In less than one year, Zhang and his organization laundered at least $25 million.

A large portion of the laundered funds were generated by criminal groups operating overseas who tricked U.S. victims into falling for a variety of internet-based frauds. These frauds included tricking victims into sending money to purchase or extend warranties or soliciting victims to invest in cryptocurrencies and then stealing the invested funds. In order to help these criminal groups launder these funds, Zhang needed U.S. bank accounts.

Rongjian Li was a Bank of America employee in New York who became friendly with Zhang. In 2021-2022, Zhang directed his runners to meet with Li at Li's Bank of America branch. Li knew some of Zhang's accounts were opened with runners using fraudulent passports and knew that the accounts were intended for use to launder "scam" money. When the bank's financial auditing systems flagged or froze accounts for suspicious activity, Li misused the branch customer information system to help Zhang move illicit funds elsewhere. Finally, Li was seated next to Zhang at a lengthy recorded dinner in New York with undercover agents where Zhang discussed the different fee percentages he charged various criminal groups for drug trafficking and scams. (Source)

Credit Union Manager Sentenced To Prison For Embezzling $770,000+ Over 14 Years - November 6, 2025

For 30 years, Rita Hartman was the manager of Muddy River Credit Union (Formerly Atchison Casting Credit Union & Bradken Federal Credit Union), in Kansas which served the employees of a foundry located in Atchison, Kansas. Hartman's position gave her control over all aspects of Muddy River's finances.

Between 2007 and 2021, she abused the trust that Muddy River granted her to steal approximately $346,00 in customer cash deposits. Hartman also fraudulently credited approximately $430,000 in deposits and loan payments to her or her relatives' accounts when no payments or deposits had been made. Hartman concealed her conduct by altering ledgers and records and by falsifying information submitted to Muddy River's regulators. She obstructed efforts to uncover her fraud by submitting fraudulent documents to regulators and delaying a mandated audit.

The defendant's embezzlement wiped out Muddy River's capital and rendered it insolvent, ultimately forcing a merger into another credit union to continue operations.

In 2013, the then-Governor of the State of Kansas appointed Hartman to the Kansas Credit Union Council, which advises the Kansas Department of Credit Unions on issues and needs of credit unions. Hartman is also a former mayor and city commissioner in Atchison.

A federal judge ordered that during her imprisonment, all of Hartman's state pension payments be directed towards the $778,361 in restitution she was ordered to pay as part of her sentence. (Source)

Bank Employee Sentenced To Prison For Embezzling $280,000 From Bank Vault - November 14, 2025
Jennifer Lamanna worked for an FDIC-insured financial institution.

Over a period of months, Lamanna embezzled $280,000 from the institution by stealing funds from the bank vault. After embezzling the funds, Lamanna deposited the majority of funds into a bank account under her control. To balance out the vault and conceal her embezzlement, Lamanna made multiple large withdrawals and subsequent matching deposits out of a customer's account. To make the sham transactions appear legitimate, Lamanna filed fictitious Currency Transaction Reports (CTR).

On June 8, 2023, Lamanna made a materially false statement to the Financial Crimes Enforcement Network, a sub-agency of the U.S. Treasury Department, when she completed and submitted a CTR falsely stating that a bank customer deposited $160,100 in cash into his account knowing that no such deposit took place. (Source)

PHARMACEUTICAL COMPANINES / PHARMICIES / HOSPITALS / HEALTHCARE CENTERS / DOCTORS OFFICES / ASSISTED LIVING FACILITIES
No Incidents To Report

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION
Palantir Technologies Suing 2 Former AI Engineers For Stealing Trade Secrets Worth BILLIONS Of Dollars - October 30, 2025
Palantir Technologies has filed a lawsuit against two former senior artificial intelligence (AI) engineers, Radha Jain and Joanna Cohen. In a lawsuit filed in Manhattan federal court, the defense tech company has alleged that they stole confidential documents and information to help establish a "copycat" competitor named Percepta. Palantir said that both women had access to the company's most valuable assets, including its source code, which it claims to have invested billions of dollars in.

Palantir highlighted the engineers had significant roles in the company, stating, "Jain and Cohen were far from rank-and-file employees." The company further detailed their responsibilities, noting, "Jain designed and built Palantir's flagship software, and Cohen interacted directly with some of Palantir's largest and most important customers."Palantir claims that Jain and Cohen engaged in deception over several months and provided false information about their intentions when they resigned in November 2024 and February 2025, respectively. The company also alleges that Cohen took "highly confidential documents" the day before her departure by sending them to herself via Slack.

Palantir referred to Percepta as a "copycat competitor," pointing out that Percepta's chief executive officer and many other executives are also former employees of the company. Palantir asserts that Jain and Cohen have provided Percepta with an illegal "head start" in developing a rival business. " (Source)

Vice President Of Qualcomm's Research & Development Department Sentenced To Prison For $180 Million Technology Fraud Scheme - November 14, 2025

Dr. Karim Arabi was sentenced in federal court to 48 months in prison for wire fraud and money laundering in connection with a massive $180 million scheme targeting his then-employer, Qualcomm.

Dr. Arabi was ordered to forfeit more than $45 million plus properties in Canada and Norway, and to pay $100,894,711.12 in restitution to Qualcomm.

While working as a Vice President of Qualcomm's Research and Development Department, Dr. Arabi committed fraud by developing valuable microchip technology, marketing the technology through a company,

Abreezio, which he created to conceal his involvement, and then selling the company and its technology to Qualcomm for $180 million. In reality, Qualcomm would not have paid a dime for the technology had it known of Dr. Arabi's involvement because, as part of his employment with Qualcomm, Dr. Arabi had agreed that virtually all technology he invented while working at Qualcomm belonged to his employer.

Dr. Arabi and his accomplices created a host of lies and false documents to deceive Qualcomm about Abreezio's origins. Dr. Arabi himself created two fake email accounts to impersonate his sister to make it appear that she was actively participating in Abreezio and to hide his own involvement.

His accomplices repeatedly called him by his sister's name in their communications to obscure his role. Dr. Arabi even created a fake resume for his sister, embellishing her background to make it more plausible that a graduate student could have invented the technology behind a $180 million company. (Source)

Federal Lawsuit Alleges Theft Of Trade Secrets By Former Engineers To Start Competing Company - November 10, 2025

On November 7, Columbus-based Best Lighting Products Inc., a longtime supplier in the North American emergency lighting market, filed a federal lawsuit in that reads less like a business dispute and more like a tale of corporate espionage.

The 9-page complaint accuses former engineering managers at Best Lighting's factory in China, now operating under the QLLITE brand, of orchestrating an elaborate scheme to clone and rebrand Best Lighting's products using the company's own proprietary tooling and trade secrets. The suit names four defendants, including a New Jersey-based importer and two China-based engineers, and alleges theft, deception, and a transpacific game of hide-and-seek.

2 of Best Lighting's former engineering managers in China — Wang Jinhong and Jin Tao — quietly launched a competing company, Wanju Electronics, while still on the payroll of Best Electronics Technology Co., Ltd., a wholly owned subsidiary of Best Lighting. Not only did they allegedly divert factory workers to moonlight on rival products, but they're also accused of using Best Lighting's own molds to manufacture knockoff emergency lighting units.

Once built, those lookalike products, the complaint claims, were funneled into the U.S. through a New Jersey-based company called Mega Safety Industries, which is allegedly tied to the individual defendants. The products appear on Amazon and Walmart under the brand name QLLITE. As Best Lighting tells it, this was no accidental resemblance — the cloned items are so similar, they might as well have been stamped "Made by Us" with a Sharpie. (Source)

Google Is Investigating A Security Breach Involving A Google Contractor Who Exfiltrated Nearly 2,000 Screenshots & Sensitive Internal Files - October 26, 2025

Google is currently investigating a significant security breach involving a contractor who systematically exfiltrated nearly 2,000 screenshots and sensitive internal files over several weeks in October 2025. The compromised data includes critical information about Google Play Store infrastructure, security guardrails, and protective systems that underpin one of the tech giant's most valuable revenue streams. This incident represents the latest chapter in a troubling pattern of insider threats that have plagued Google over the past decade, exposing vulnerabilities in contractor oversight and access management protocols.

Google discovered that a contractor with legitimate system access had been methodically capturing screenshots and downloading confidential files related to the Play Store ecosystem.

The breach unfolded over multiple weeks before detection, allowing the perpetrator significant time to accumulate sensitive technical documentation.

The compromised materials reportedly include detailed information about Play Store infrastructure components, security mechanisms designed to protect the marketplace from malicious apps, and internal guardrails that ensure compliance with global regulations. Given that the Play Store serves billions of Android users worldwide and represents a cornerstone of Google's mobile ecosystem, the exposure of these systems creates substantial risk for potential exploitation by adversaries." (Source)

TSMC Executive Faces Taiwan Legal Investigation For Providing Trade Secrets To Intel - November 18, 2025

Taiwanese authorities have opened a national-security-related inquiry involving a former TSMC R&D executive who may have passed the company's trade secrets to a foreign company. The person in question is Wei-Jen Lo. The investigation is focused on finding out whether there was an intentional or unlawful transfer of TSMC's trade secrets to a foreign entity.

Wei-Jen Lo, a long-time executive at TSMC and Intel, this year retired from the Taiwanese foundry giant after spending 21 years at the company and building one of the strongest semiconductor R&D teams in the industry. However, instead of enjoying life, he unexpectedly surfaced at Intel in late October. Furthermore, he allegedly took a large collection of confidential materials related to TSMC's leading-edge process technologies with him.

Wei-Jen Lo reportedly rejoined Intel as 'vice president of R&D' in late October, about three months after departing TSMC. But before leaving TSMC, Lo allegedly used his authority as the senior vice president of corporate strategy development to instruct subordinates to provide him copies of restricted technical documents covering TSMC's N2, A16, A14, and post-A14 process technologies and their derivatives. Since Lo was a high-ranking executive, such requests appeared routine, so no internal security flags were raised at the time. (Source)

Intel Files Lawsuit Against Former Employee Who Stole 18,000 Files From Internal Database

Intel is experiencing an incident of 'information theft' by one of its former employee, who has allegedly stolen 'top secret' data, despite being with the company for more than a decade.

Well, it appears that the latest round of layoffs within Intel has 'pissed' off an employee, who has stolen sensitive data from the firm. The employee, named Jinfeng Luo, is reported to have been with Intel since 2014 and had recently received a layoff notice, which terminated his employment as of July 31st.

It is said that during his last days, Luo had stolen around 18,000 files from Intel's internal database, which included "top secret" data.

After the 'shady' file transfer attempt, Intel looked into the matter and started an investigation, which found Luo to be the perpetrator. Intel is demanding $250,000 in damages and a court order to ensure that Luo doesn't leak out sensitive information. (Source)

Apple Engineer Stole Apple Watch Trade Secrets And Then Gave Presentation To 100 Employess At His New China Employer - October 28, 2025

Chinese smartphone maker Oppo recruited a former Apple Watch engineer who stole trade secret information from Apple and then gave a presentation on that data to hundreds of Oppo employees.

Apple has accused former employee Chen Shi of stealing Apple Watch trade secrets to provide to Oppo.

The two companies have been battling it out in court. Apple claims that Oppo is withholding information, while Oppo says no trade secrets were disclosed.

Apple discovered that Shi gave a presentation on Apple sensor technology, providing insight into Apple's sensor development and future product plans.

Internal Oppo communications promoted an "Apple Sensors" talk with Shi, titled "Apple's Sensor Hardware R&D Philosophy and Methodology." A tagline for the meeting said "Are you curious about how Apple's sensors are developed?"

Apple claims that Shi's presentation included slides taken directly from materials procured from Apple, and that he answered specific questions about sensor design at Apple. Oppo is accused of encouraging Shi to share the trade secret information.

Prior to leaving Apple, Shi downloaded 63 files from Apple's protected Box folder and transferred them to a USB drive, then he searched for information on how to cover his tracks. Shi also reportedly attended "dozens" of one-on-one meetings with Apple Watch technical team members to learn about their research before he left the company. (Source)

General Manager For U.S. Defense Contractor L3Harris Pleads Guilty To Stealing & Selling Trade Secrets To Russian Broker - October 30, 2025

Peter Williams, 39, pleaded guilty to stealing and selling his employer’s trade secrets to a Russian cyber-tools broker. Williams worked as a director and general manager at L3Harris' Trenchant division, which develops cyber weapons.

The trade secrets were stolen over a three-year period from the U.S. defense contractor where he worked. The trade secrets were comprised of national-security focused software that included at least eight sensitive and protected cyber-exploit components.

Those components were meant to be sold exclusively to the U.S. government and select allies. Williams sold the trade secrets to a Russian cyber-tools broker that publicly advertises itself as a reseller of cyber exploits to various customers, including the Russian government.

Willaims admitted from approximately 2022 through 2025, he improperly used his access to the defense contractor’s secure network to steal the cyber exploit components that constituted the trade secrets.

Williams resold those components in exchange for the promise of millions of dollars in cryptocurrency. To effectuate these sales, Williams entered into multiple written contracts with the Russian broker, which involved payment for the initial sale of the components, and additional periodic payments for follow-on support. Williams transferred the eight components and trade secrets to the Russian broker through encrypted means. He used the proceeds to buy himself high-value items. (Source)

Aviation Company Files Lawsuit Against Former Employee For Theft Of Trade Secrets - November 22, 2025

Joby Aviation has filed a lawsuit in California's Santa Cruz County Superior Court accusing rival Archer Aviation of corporate espionage and theft of trade secrets. The complaint states that Archer hired Joby's former US state and local policy lead, George Kivork, who shortly before resigning allegedly downloaded dozens of confidential files and forwarded some to his personal email.

Reuters reports that the leaked documents included business strategies, partnership terms, aircraft specifications and vertiport-development plans. Joby alleges Archer used this information to interfere with an exclusive infrastructure deal involving a real-estate developer. Archer has denied the allegations, calling the suit unfounded and an attempt to stifle competition. (Source)

Cannabis Company Suing Former Employee For Stealing Trade Secrets Worth $750,000 - October 19, 2025

New Jersey-based cannabis products manufacturer, Kushi Labs LLC, has filed a federal lawsuit against its former employees, alleging that they unlawfully took confidential trade secrets to a competitor, seeking damages of at least $750,000.

The company accuses the ex-employees of misappropriating valuable trade secrets and using them for the benefit of a rival manufacturer. (Source)

Company Suing Former Consultant For Stealing Trade Secrets - October 8, 2025

Autonomous delivery receptacle company Arrive AI Inc. is suing a former consultant, alleging he stole trade secrets and is sabotaging a business opportunity that Arrive was working on with a top logistics company.

The complaint says that Myron Wright and his company, Wright Flyer Consulting Group Inc., must cease using the technical information related to Arrive's delivery systems and return all confidential materials.

The suit also says Wright should be found liable for frustrating a deal, identified in the complaint as "Project Astro," by hiring departing employees from the project's target customer.

Wright directed his new employees not to work with Arrive, causing the project to continually be postponed, the suit says.

"Given the delays caused by Wright and competitors in the industry, Arrive is on the brink of losing what could be a multibillion-dollar deal," Arrive says.

Arrive, an Indiana company founded in 2019, makes temperature-controlled vaults, or smart mailboxes, called "Arrive Points."

Courier companies can drop packages via drone into these mailboxes and customers can retrieve them using radio frequency identification or a personal identification number, according to the company's website.

The company hired Wright in October 2022 to help foster a relationship with one of the world's top logistics companies for Project Astro. Because he was a former employee of the unnamed logistics company, he was brought on to help tailor Arrive's product offerings to meet that company's needs, the suit says.

As a consultant, Wright sat in on board meetings and gained knowledge of the company's patents and proprietary trade secrets. Those secrets include information that exceeds the scope of its patents such as financial data, key vendor contacts and specific RFID technology, according to the complaint.

Arrive terminated its agreement with Wright on Jan. 2. The suit alleges that he then shared the company's confidential information with multiple competitors, costing Arrive millions of dollars in potential revenue. (Source)

CrowdStrike Terminates Insider For Leaking Internal Data To Hackers For $25,00 Payment - November 22, 2025

Cybersecurity giant CrowdStrike has officially confirmed the termination of an employee who was caught providing sensitive internal system details to a notorious hacking collective.

The incident came to light when internal screenshots appeared on a public Telegram channel managed by the threat group known as “Scattered Lapsus$ Hunters.”

This group describes itself as a “supergroup” formed by members of Scattered Spider, LAPSUS$, and ShinyHunters, and posted images claiming they had successfully accessed CrowdStrike’s internal environment.

The leaked images, reviewed by researchers, showed internal dashboards and an Okta Single Sign-On (SSO) panel that employees use to access corporate applications.

According to reports the hackers approached the insider and allegedly offered $25,000 to facilitate access to the network.

"We identified and terminated a suspicious insider last month following an internal investigation that determined he shared pictures of his computer screen externally," a CrowdStrike spokesperson stated. Our systems were never compromised and customers remained protected throughout. We have turned the case over to relevant law enforcement agencies." (Source)

ARTIFICIAL INTELLIGENCE (AI) INSIDER THREATS

65% Of Leading AI Companies Expose Verified Secrets Including Keys And Tokens On GitHub - November 11, 2025

A new security investigation reveals that 65% of prominent AI companies have leaked verified secrets on GitHub, exposing API keys, tokens, and sensitive credentials that could compromise their operations and intellectual property.

The Wiz research, which examined 50 leading AI companies from the Forbes AI 50 list, uncovered widespread security vulnerabilities across the industry.

These leaked secrets were discovered in deleted forks, gists, and developer repositories, representing an attack surface that standard GitHub scanning tools routinely overlook. Among the most impactful leaks were Langsmith API keys granting organization-level access and enterprise-tier credentials from ElevenLabs, discovered in plaintext configuration files.

65% of exposed companies were valued at over $400 billion collectively. Yet, smaller organizations proved equally vulnerable, even those with minimal public repositories demonstrated exposure risks.

Wiz experts emphasize the urgent need for action by AI companies. Implementing mandatory secret scanning for public version-control systems is essential and cannot be overlooked. (Source)

How Artificial Intelligence Is Turning Employees Into Unwitting Insider Threats - November 14, 2025

It might look like a harmless request: "summarize the attached financial report and point out any potential compliance issues." Within seconds, a generative AI tool delivers a neatly packaged analysis that saves hours of work. What feels like productivity, however, is actually exposure: by pasting a sensitive document into a public AI model, an employee has unknowingly smuggled confidential data beyond the organization's walls.

This isn't the work of malicious insiders, but of well-intentioned staff simply trying to work faster and smarter. Yet the scale is staggering – nearly 1 in 20 enterprise users now rely on GenAI, with sensitive data flowing into these platforms 30 times more year-on-year. Worse still, 72% of this shadow AI use happens outside IT's control, leaving organizations blind to the modern equivalent of opening Troy's gates.

There are even greater dangers than copying and pasting data into GenAI tools. Risks including prompt injection attacks – where hidden commands are embedded in documents or queries that can co-opt systems into ignoring security protocols or sharing confidential information. Other hidden problems include: context hijacking, data poisoning, and LLM memory persistence, where cached queries or context reuse could expose sensitive information to subsequent users.

Importantly, there are real-world exploits. Security researchers from University of California, San Diego (UCSD) and Nanyang Technological University in Singapore unveiled a new attack that covertly instructs an LLM to harvest sensitive information. This includes names, ID numbers, payment details, email and postal addresses, which can be sent directly to a hacker. Dubbed "Imprompter", the attack relies on an algorithm that turns a user's prompt into hidden malicious commands, achieving close to an 80% success rate in extracting personal data through obfuscated prompts. (Source)

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

U.S. Think Tank Waves Red Flags Over Chinese Economic Espionage And Insider Threats - November 11, 2025

"China's campaign of economic espionage against the United States spans cyber intrusions, insider theft, and technology transfer disguised as collaboration," declared the report written by intelligence analyst and applied historian Darren E. Tromblay and published by the Information Technology & Innovation Foundation (ITIF).

A call to disrupt the People's Republic of China's economic espionage campaign against the United States was sounded in a new report by a Washington, D.C., technology think tank.

China's approach to espionage is more than spycraft. It's an entire ecosystem. The Chinese system is fundamentally different from other U.S. adversaries in both scale and integration, observed Michael Bell, CEO of Suzu Testing, a provider of AI-powered cybersecurity services, in Las Vegas.

"Russia conducts opportunistic espionage through intelligence services," he told TechNewsWorld. "China operates a whole-of-society approach where companies, universities, and talent programs function as coordinated collection platforms."

"Based on the cases we've been seeing and industry analysis, no other nation-state has achieved the level of integration where a student visa, university partnership, and a state-owned enterprise investment can all be vectors for the same operation," he said.

Why Insider Access Is So Damaging

April Lenhard, principal product manager for cyber threat intelligence at Qualys, a provider of cloud-based IT, security, and compliance solutions, in Foster City, Calif., explained that insider threats are so damaging because employees already know how to navigate systems that are gated off to outsiders.

"Trusted employees don't just steal files," she told TechNewsWorld. "They also know to take and use processes, context, and proprietary 'secret sauce' that costs American companies billions of dollars in R&D, while handing it over to China for free. That innovation can't be recovered once it's gone."

Insider threats are uniquely damaging because they often bypass many traditional perimeter-focused defenses, added Eran Barak, co-founder and CEO of MIND, a platform focused on data loss prevention and insider risk management, in Seattle.

"Whether intentional or accidental, insiders already have access to sensitive systems and data," he told TechNewsWorld. "That access, combined with a lack of visibility and control, makes it easier to exfiltrate critical information without triggering alerts."

"Nation-state actors often exploit this by targeting individuals with privileged access, knowing that human behavior is more difficult to monitor than external network traffic," he continued.

"According to industry research, data sprawl, alert fatigue, and lack of contextual awareness in legacy security systems have made insider threats not only harder to detect, but also more impactful when successful." "The reality is, adversaries don't need to break in if they can log in," he said. (Source)

Engineer Sentenced To Prison For Stealing Trade Secret Technology Designed For Missile Launch And Detection For People's Republic Of China Government - November 17, 2025

Chenguang Gong is a former engineer at a Southern California company. He is a dual citizen of the United States and China/

Gong pleaded guilty to stealing trade secret technologies developed for use by the U.S. government to detect nuclear missile launches, track ballistic and hypersonic missiles, and to allow U.S. fighter planes to detect and evade heat-seeking missiles. Gong transferred more than 3,600 files from a Los Angeles-area research and development company where he worked to a personal storage devices during his brief tenure with the company in 2023.

The files Gong transferred include blueprints for sophisticated infrared sensors designed for use in space-based systems to detect nuclear missile launches and track ballistic and hypersonic missiles, as well as blueprints for sensors designed to enable U.S. military aircraft to detect incoming heat-seeking missiles and take countermeasures, including by jamming the missiles' infrared tracking ability. Some of these files were later found on storage devices seized from Gong's temporary residence. Oaks.

Law enforcement also discovered that, between approximately 2014 and 2022, while employed at several major technology companies in the United States, Gong submitted numerous applications to 'Talent Programs' administered by the People's Republic of China (PRC) government. (Source)

Fibre Optics Engineer Convicted Of Stealing DARPA Trade Secrets For China's Thousand Talents Plan - November 5, 2025

On or about July 1, 2016, Ji Wang stole hundreds of files that contained non-public data generated during the DARPA project, including trade-secret manufacturing technology that would have enabled him to fabricate all manner of specialty optical fibers, including for fiber lasers.

Ten days before Wang stole the trade secret files, he had applied for China's Thousand Talents Plan Award. The Thousand Talents Plan Award was an initiative by the Chinese government aimed at people who were born in China and immigrated to the United States, to study or work in science and technology fields. The Thousand Talents Plan Award incentivized these people to return to China by promising millions of dollars of investment to award recipients who returned to China. Two months after Wang stole the trade secret files, he was selected to receive a Thousand Talents Plan Award.

Wang was negotiating with Chinese government entities to start a specialty fiber business in China from at least 2014 through 2017. Wang was negotiating to receive tens of millions of dollars in investment from Chinese government entities, who would have been shareholders in his new venture.

Wang's business plans showed that he was planning to use the stolen trade-secret files to start this business in China. Wang's business plans also touted the military applications of the technology.

In one such business plan, which Wang submitted to a Chinese government entity, he advertised that specialty fibers "can also be installed on military vehicles," including "tanks."

Wang claimed that such use of the technology on military vehicles could "be key to deciding victory or defeat." Ultimately, law enforcement disrupted Wang's efforts before he was able to start a new business and exploit the technology he stole. (Source)

North Korea's IT Fraudulent U.S Workers Program Are Now Targeting Other Industries Such As Finance, Healthcare, Public Administration & Professional Services - October 1, 2025

North Korea's (DPRK) clandestine IT Worker (ITW) program, which is long known for targeting U.S. technology firms and crypto firms, has broadened its scope to attempt to infiltrate a variety of industries worldwide, including finance, healthcare, public administration, and professional services.

Okta's threat researchers have identified over 130 identities associated with DPRK linked facilitators and workers, which collectively pursued more than 6,500 interviews across 5,000+ companies until mid-2025, and have found that the threat is far more pervasive: 50% of targeted entities are not technology companies, and 27% of them lie outside of the United States.

Organizations in every vertical offering remote or hybrid roles are now potential targets. Beyond payroll diversion, successful placements allow these workers to access to sensitive systems and networks, opening the door to data exfiltration, extortion, or intelligence gathering, DPRK IT Workers aren't just applying for coding roles anymore: they are increasingly targeting finance, payments processing, and engineering support positions.

To read how to protect your company from this serious threat, read the rest of the story. (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

2 Chief Executive Officers For Primary Health Network Plead Guilty To $1.7 Million Kickback Fraud Scheme - November 14, 2025

2 former Chief Executive Officers and a former facility manager for Primary Health Network (PHN) have pleaded guilty in federal court to charges of agreeing to defraud their former employer.

Drew Pierce, 58, Jack Laeng, and Mark Marriott, 58, pleaded guilty to conspiracy to commit wire fraud and conspiracy to commit money laundering.

In connection with the guilty pleas, the Court was advised that PHN was a non-profit organization in Sharon, Pennsylvania, that provided medical services to patients in underserved parts of Pennsylvania, regardless of their ability to pay. From approximately July 2015 through January 2019, Pierce served as CEO of PHN, Laeng as former CEO, and Marriott as the company's facilities manager. The three defendants and others agreed to insert a company called TopCoat, which they owned, between PHN and third parties, with TopCoat paying the third party for providing a service for PHN, then billing PHN a higher amount so that TopCoat could profit.

Marriott caused fraudulent invoices to be issued from TopCoat to PHN, purporting that TopCoat had done work when it in fact had not.

Pierce, Laeng, Marriott, and others split the profits—the difference between what PHN paid TopCoat and what TopCoat paid the third parties—among themselves, including by issuing checks from the TopCoat bank account to themselves or other entities they controlled. On one deal alone in 2017, TopCoat received more than $200,000 additional from PHN than what it paid the true vendor on a project.

Pierce, Laeng, and others also agreed to defraud PHN through a separate scheme in which the conspirators caused PHN to enter into contracts with a third party in exchange for the third party paying 50% of the fees received to an entity controlled by Pierce, Laeng, and their co-conspirator.

In all, Pierce, Laeng and their co-conspirator received more than $1.7 million in kickback payments from the third party between 2013 and 2020, the proceeds of which they split among themselves. (Source)

President & Chief Operating Officer Of Public Company Pleads Guilty To Insider Trading / He Made Profits Of $145,000+ - November 18, 2025

Michael Smith, 48, served as the President and Chief Operating Officer of Company-1 since in or around June 2022. Company-1 was based in Idaho, and its shares were publicly traded on NASDAQ.

By at least June 2024, by virtue of his position at Company-1, Smith received material nonpublic information (MNPI) regarding the impending acquisition of Company-1 by another company. Smith was subject to Company-1's Insider Trading Policy that, among other things, prohibited employees from trading in Company-1's stock if an employee possessed MNPI.

On July 26, 2024, Smith bought Company-1 stock using a brokerage account belonging to Individual-A. Smith and Individual-A had a close personal relationship. Smith executed these trades on the basis of MNPI about the impending acquisition of Company-1 despite knowing that he was prohibited from trading Company-1 stock.

On Aug. 7, 2024, news of Company-1's acquisition became public, and Company-1's stock increased by nearly 50%. The next day, Smith sold the Company-1 stock he had purchased for Individual-A for a profit of approximately $145,754.69. Smith executed the trades to financially benefit Individual-A. (Source)

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

Former Sig Sauer Employee Indicted For Re-Selling Hundreds Of Guns Bought With Company Discount - November 17, 2025

Patrick Goulet, a former machinist for New Hampshire-based gun manufacturer Sig Sauer is facing federal wire fraud and firearms charges after allegedly using his employee discount to purchase and then resell guns without a license. Goulet worked at Sig Sauer until he was fired by the company in 2023.

He also used the names of fellow co-workers to acquire additional Sig Sauer products at steep discounts, before reselling the weapons online.

Between August 2021 and June 2024, the Bureau of Alcohol, Firearms and Tobacco alleges Goulet sold several hundred guns to customers nationwide, though he did not have a license to deal firearms. Goulet used social media platforms such as Facebook to locate persons interested in buying discounted firearms."

The gunmaker offers its employees deep discounts on a limited number of firearms. However, the manufacturer prohibited its employees from selling or otherwise using the discount for personal profit. (Source)

Chief Executive Officer For Large Steel Manufacturer Charged In $66 Million Fraud Scheme / Used Funds For Extravagant Lifestyle - November 18, 2025

From at least in or about October 2022 through in or about August 2024, Derek Wachob who was the Chief Executive Officer of a large manufacturer of steel pipes based in Sapulpa, Oklahoma (Company1),
engaged in a scheme to defraud individual investors, a bank, an investment firm, and at least two steel pipe distributors of at least $66 million.

To obtain money from each of the victims, Wachob lied and misled the victims by, among other things, falsely claiming to offer purported business opportunities based on future steel purchases that Wachob pledged to make. Wachob used these misrepresentations to take millions of dollars from even some of his closest friends.

Instead of using the victims' money as promised, Wachob spent the funds to maintain his extravagant lifestyle of expensive cars, vacation homes, private jets, helicopters, and yachts, and prop up Company-1, which was struggling financially and in debt. (Source)

Chief Financial Officer For Seafood Wholesaler Sentenced To Prison For Embezzling $9 Million+ Over 5 Years / Used Funds To Purchase Luxury Goods - November 17, 2025

From at least 2015 and continuing into 2020, Antonietta Nguyen misappropriated approximately $2.7 million in company funds.

Nguyen used her access to ABS Seafood's bank account and credit cards to divert millions of dollars to pay off her personal credit card, pay personal expenses on her corporate credit card, and authorize payment of fraudulent invoices from a seafood exporter in the Philippines that was formally owned by Nguyen's brother.

Nguyen used the stolen funds to pay property taxes for her residence and a rental property, her children's college tuition, and over a million dollars in luxury goods, among other expenses.

Nguyen traveled the world to purchase luxury purses, scarves, and other items, which she stored in a designated room in her home. She also provided corporate credit cards to her family members and authorized charges including luxury vacations that were ultimately paid for by ABS Seafood. (Source)

Office Manager Pleads Guilty To Embezzling $1.7 Million+ By Forging Business Owner's Signature On Checks 500 Timees Over 8 Years / Used Funds For Personal Enrichment - September 30, 2025

Tammy Barcus is the former office manager and bookkeeper for an Ocean City based home builder in Maryland.

Barcus admitted to embezzling at least $1,790,000 from her former employer. She forged a business owner's signature on business checks at least 500 times. Barcus then concealed the embezzlement from her employer and the Internal Revenue Service (IRS) by making false entries into the business' books and records.

From 2016 through 2024, Barcus used her position of trust to embezzle money by issuing more than 500 fraudulently authorized checks from the home builder's business bank account.

Barcus forged the signature of one of the owners on the face of the business checks and then deposited the checks into bank accounts she controlled. She then used the money for her personal enrichment.

The former office manager and bookkeeper concealed the scheme by hiding the embezzled income from the IRS.

She also made materially false and fraudulent edits and entries into the home builder's internal accounting records to cover up the fraudulent payments and commingled the embezzled funds into a bank account she controlled. (Source)

Office Manager Convicted Of Embezzling $1.4 Million / Used Funds To Pay Down Balances On Personal Credit Cards, Purchase 2 Houses, Cars, Etc. - November 19, 2025

Between November 2019 and May 2023, Kami Power worked as an office manager and controller at a family-owned construction company in South Lake Tahoe.

During her employment, Power embezzled more than $1.4 million from the company.

She disguised more than $700,000 of these fraudulent transfers as payments made to vendors that the company worked with—under fake profiles she created in the names of real companies, as well as fake companies that reflected her own initials, such as "KEP Inc. Sale" and "KPI." She disguised additional fraudulent transfers as payments for payroll or reimbursements.

Power also used the company's credit card to make unauthorized personal purchases and paid down the balance of her own personal credit cards. Power used the money she stole to purchase two houses, several new cars and ATVs, and a horse. She also spent the money on field-level seats at football games and a $29,000 Hawaii vacation. (Source)

Chief Financial Officer Charged With Embezzling $700,000 - November 17, 2025

Pamela Aguilar was employed as Chief Financial Officer of a Connecticut software company.

Between approximately 2018 and 2025, Aguilar defrauded her company by making ACH and wire transfers from her company's account to personal bank accounts, writing checks and making cash withdrawals from her company's account, and by making PayPal and credit card payments from her company's account for her own benefit.

It is alleged that through this scheme, Aguila stole approximately $700,000 from Company A. Aguilar attempted to cover up her criminal behavior by providing false weekly cash reports and false monthly financial statements to company's Chief Executive Officer. (Source)

Former Administrative Professional For Company Admits Embezzling $615,000+ / Used Funds For Rent, Utility Bills, Car Repairs, Etc. - November 20, 2025

Crystal Halbert admitted in a plea agreement that she misappropriated the money from 2015 to 2023 while holding various administrative positions in the company's Corporate Governance function and the Office of the Chief Executive Officer.

Lyon-Halbert directed company funds to her personal bank account and made a series of unauthorized credit card purchases for her personal benefit, including storage rental space, rent payments, personal utility bills, car rentals, auto shop bills, clothing, furniture, and other items.

Halbert concealed her misappropriation by falsely representing that the credit card payments were directed to vendors that had provided services to the company, the plea agreement states. (Source)

Office Manager Pleads Guilty To Embezzling $400,000+ From Employer / Used Fund For Vacations, Country Club Memberships, Etc. - November 13, 2025

Between December 2019 and March 2025, Marie Hobson inflated her own payroll by adding approximately $268,046 in phony expense reimbursements, such as uniform costs even though Hobson did not wear a uniform in her position.

To conceal the thefts, Hobson manipulated her employer's accounting software to make it appear she was only receiving her weekly salary. Hobson also misused her company-issued credit card to pay for country club memberships, vacations, cruises, timeshares and personal residence costs totaling more than $105,000. (Source)

Company Payroll Manager Admits To Embezzling $305,000 - November 13, 2025

Deborah Stinebaker, 49, admitted that while the head of the company's payroll department, she used the company's financial software to pay herself an extra $305,469 from January 2016 to March of 2024.

Her employer discovered her crime when an audit revealed that the company's financial instability resulted from the embezzlement. (Source)

Financial Secretary Pleads Guilty To Embezzling $54,000+ From Brotherhood Of Railroad Signalmen Union / Used Funds To Pay Personal Credit Cards, Etc. - November 25, 2025

David Scofield is the former recording financial secretary for the Brotherhood of Railroad Signalmen, AFL-CIO, Local Lodge 21 (BRS Local Lodge 21), pleaded guilty in federal court yesterday to embezzling nearly $55,000 from the labor union.

Scofield was an officer of BRS, having been elected to that position in or about 2005, and holding that position until in or about November 2023. In that capacity, Scofield had access to BRS Local Lodge 21's bank account and was authorized to use the checking account only for BRS Local Lodge 21's expenses.

Scofield admitted that he used BRS Local Lodge 21's bank account to make $54,412.67 in personal expenditures, including expenditures for the payment of his personal PayPal account, personal credit cards, and personal loans. (Source)

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

No Incidents To Report

SHELL COMPANIES / FRAUDULENT INVOICE BILLING SCHEMES

2 Pilots Charged For Providing Fake Invoices To Their Employer And Fraudulently Obtaining $785,000 From Over Billing Scheme - November 14, 2025

Between October 10, 2021, and July 27, 2023, Jean Paul Romero and Jordan Coursey knowingly devised a scheme to defraud their employer, Constellation Productions, Inc. Constellation is an aviation and production company in Marion County, Florida.

It was part of their scheme that the two pilots personally paid the costs to fuel Constellation aircraft.

They then created false invoices with material misrepresentations that overstated the fueling costs and electronically submitted them by email to Constellation for reimbursement. Romero and Coursey y obtained a total of $785,050 from this over billing scheme. (Source)

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

Employee Charged For Sabotaging Employers Network For 1 Year After Being Terminated / Caused Widespread Disruption To The Company Operations - November 20, 2025

Ezekiel Potter, 34, after being terminated by his employer in April 2023, accessed or attempted to access to the employer's computer systems without the employer's authorization.

When he gained access, Potter reset usernames and passwords for the employer's accounts and deleted or revoked access to employer's accounts.

Potter engaged in this conduct for over a year and a half—from May 14, 2023, until at least January 16, 2025. Potter's actions caused widespread disruption to the employer's operations and resulted in tens of thousands of dollars in losses to the employer. (Source)

Disgruntled Employee Sentenced To Prison For Remotely Releasing Toxic Chemicals Into Chicken Plant After Being Fired - November 6, 2025

William Taylor, 52, pleaded guilty to repeatedly logging into a computer system maintained by his former employee and releasing dangerous amounts of cleaning chemicals into a chicken production line in August 2023.

Taylor was fired from ChemStation after he caused a shutdown at a plant in Georgia.

Later that summer, Taylor realized that he still had access to ChemStation's system through an app on his personal phone, which gave him remote access to adjust the chemical levels at the Pilgrim's Pride chicken processing plant in Sumter, South Carolina. ChemStation used the same username and password for all of its systems, according to court filings.

Using the app, over a two-week period Taylor repeatedly changed the levels of peracetic acid and sodium hydroxide, two cleaning chemicals used in chicken production. On one occasion he caused a spike in chemicals, which "posed a potential health hazard" to workers at the plant, according to court records.

In order to cover his tracks, Taylor shut off the alarms and changed the email notification setting in the system so that no one would be alerted to the changes in chemical levels.

When confronted by FBI agents, Taylor described his actions as a "silly joke." But courts and prosecutors disagreed.

The U.S. District Court Judge who sentenced Taylor on Nov. 3, called it "an act of revenge" for his firing. On his release from federal prison, Taylor will serve another six months of house arrest while wearing an ankle monitor. He will also have to pay $5,516.26 in restitution to his former employer, ChemStation.
(Source)

Former IT Department Contractor Employee Admits To Hacking His Employer In Retaliation For Termination / Caused $862,000+ Of Damages - November 18, 2025
On May 14, 2021, Maxwell Schultz was terminated from his position as a contract employee in his company's IT department. Shortly after, he accessed the company's network by impersonating another contractor to obtain login credentials.

He ran a PowerShell script that reset approximately 2,500 passwords, locking thousands of employees and contractors out of their computers nationwide. Schultz also searched for ways to delete logs, PowerShell window events and cleared multiple system logs.

The attack to the company's system caused more than $862,000 in losses, including employee downtime, customer-service disruptions and labor needed to restore the network. (Source)

Disgruntled Employee Sentenced To Prison For Remotely Releasing Toxic Chemicals Into Chicken Plant After Being Fired - November 6, 2025
William Taylor, 52, pleaded guilty to repeatedly logging into a computer system maintained by his former employee and releasing dangerous amounts of cleaning chemicals into a chicken production line in August 2023.

Taylor was fired from ChemStation after he caused a shutdown at a plant in Georgia.

Later that summer, Taylor realized that he still had access to ChemStation's system through an app on his personal phone, which gave him remote access to adjust the chemical levels at the Pilgrim's Pride chicken processing plant in Sumter, South Carolina. ChemStation used the same username and password for all of its systems, according to court filings.

Using the app, over a two-week period Taylor repeatedly changed the levels of peracetic acid and sodium hydroxide, two cleaning chemicals used in chicken production. On one occasion he caused a spike in chemicals, which "posed a potential health hazard" to workers at the plant, according to court records.

In order to cover his tracks, Taylor shut off the alarms and changed the email notification setting in the system so that no one would be alerted to the changes in chemical levels.

When confronted by FBI agents, Taylor described his actions as a "silly joke." But courts and prosecutors disagreed. The U.S. District Court Judge who sentenced Taylor on Nov. 3, called it "an act of revenge" for his firing. On his release from federal prison, Taylor will serve another six months of house arrest while wearing an ankle monitor. He will also have to pay $5,516.26 in restitution to his former employer, ChemStation. (Source)

THEFT OF ORGANIZATIONS ASSESTS

No Incidents To Report

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

2 Facebook Vendors Plead Guilty To Conspiring With Former Facebook Diversity Program Manager To Defraud Company Of $1.2 Million - November 13, 2025

Brice Anderson and Terrance Lockett have pleaded guilty to conspiring with Barbara Furlow-Smiles, a former Diversity Program Manager at Facebook, to steal from the company. The fraud schemes involved fraudulent vendors, fictitious invoices, and cash kickbacks.

Barbara Furlow-Smiles served as Lead Strategist, Global Head of Employee Resource Groups and Diversity Engagement at Facebook, Inc. From January 2017 to September 2021, she led Diversity, Equity, and Inclusion (DEI) programs at Facebook and was responsible for developing and executing DEI initiatives, operations, and engagement programs. She later held a similar position at Nike, Inc. At both companies, Furlow-Smiles had access to corporate credit cards and was able to submit purchase requisitions and approve invoices for authorized vendors.

Furlow-Smiles used her positions at Facebook and Nike to cheat and defraud the companies.

She caused the companies to pay friends, relatives, and others associates for goods and services that were never provided, and she then directed those individuals to kick back the fraudulent proceeds to her, often in cash. Anderson and Lockett were two of the individuals who conspired with her at Facebook.

Anderson owned a business called Titan Branding LLC. Using that business, he conspired with Furlow-Smiles to fraudulently obtain nearly $1.2 million from Facebook. First, Furlow-Smiles used her Facebook credit cards to pay Titan Branding for work that was never done.

After Anderson received fraudulent payments from Facebook, he kicked back substantial sums to Furlow-Smiles.

He paid the kickbacks in cash and through transfers to accounts held in the names of Furlow-Smiles's husband and others.

Anderson sometimes wrapped cash in other items, such as T-shirts or hats, which he sent by FedEx to Furlow-Smiles. When Furlow-Smiles was in Los Angeles, California, Anderson flew there with cash and drove with Furlow-Smiles to ATMs and banks to withdraw cash to pay her.

In a separate conspiracy, Lockett conspired with Furlow-Smiles to steal over $243,000 from Facebook. Lockett hosted a podcast called the "Officially Outed Podcast" and owned a business called Officially Outed Media. Using her Facebook credit cards, Furlow-Smiles paid Lockett for services that were not provided. (Source)

EMPLOYEE DRUG & ALCOHOL RELATED INCIDENTS

Emergency Room Nurse Sentenced To Prison For Stealing Fentanyl For Patients - November 25, 2025

Travis Eskridge, 54, worked as a registered nurse in the emergency room at Ascension St. John Hospital in Michigan until August of 2022.

Eskridge admitted that he tampered with vials containing fentanyl, a powerful narcotic pain reliever, which he knew were intended to be administered to patients in the hospital's emergency room.

Eskridge removed fentanyl from the vials, replaced fentanyl with another liquid, and returned the tampered vials to the locked drug storage system. Eskridge did this with reckless disregard for the dangerous risk to patients that resulted from such tampering. Eskridge also admitted that he stole fentanyl vials as part of a pattern of thefts for his personal drug use from May of 2022 until August of 2022. Nurse Eskridge was immediately removed from his position at Ascension St. John Hospital in August of 2022 when the hospital discovered the tampering and thefts. (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'

Fired Employee Arrested For Making For Making Violent Social Media Posts Threatening To Shoot And Kill Current Employees - October 16, 2025

A former employee of Fiserv was arrested after police say she made a series of violent social media posts threatening to shoot and kill current employees.

According to a police arrest report, Anise Alvarez, 44, of Miami, was taken into custody on October 11 and charged with making written or electronic threats to kill or do bodily injury.

Investigators say Alvarez, who had been fired from her position at Fiserv, a global financial technology and payments company located in Coral Springs, Florida earlier this year, posted a string of alarming messages on her Threads account, @MZ_MAVAM, on the afternoon of her arrest. (Source)

7-Eleven Employee Arrested After Physical Altercation With Customer Results In Death - September 30, 2025

A New Brunswick 7-Eleven employee was arrested Tuesday morning following an altercation at the store that resulted in a man's death, investigators said.

Police arrived at the store at 1:40 a.m. in response to a 911 call asking for medical assistance at the George Street convenience store, according to a statement from the Middlesex County Prosecutor's Office.

Officers found Markeem Moore, 44, of Manville, unresponsive and he was rushed to Robert Wood Johnson University Hospital where he was later pronounced dead, the office said.

Detectives determined that a physical altercation occurred between Moore and the store employee, Taiwan Sanders-Boyd, 29, of New Brunswick, authorities said.

Boyd was arrested and charged with second-degree reckless manslaughter, the office said. He was being held at the Middlesex County Adult Correctional Center until his detention hearing. (Source)

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

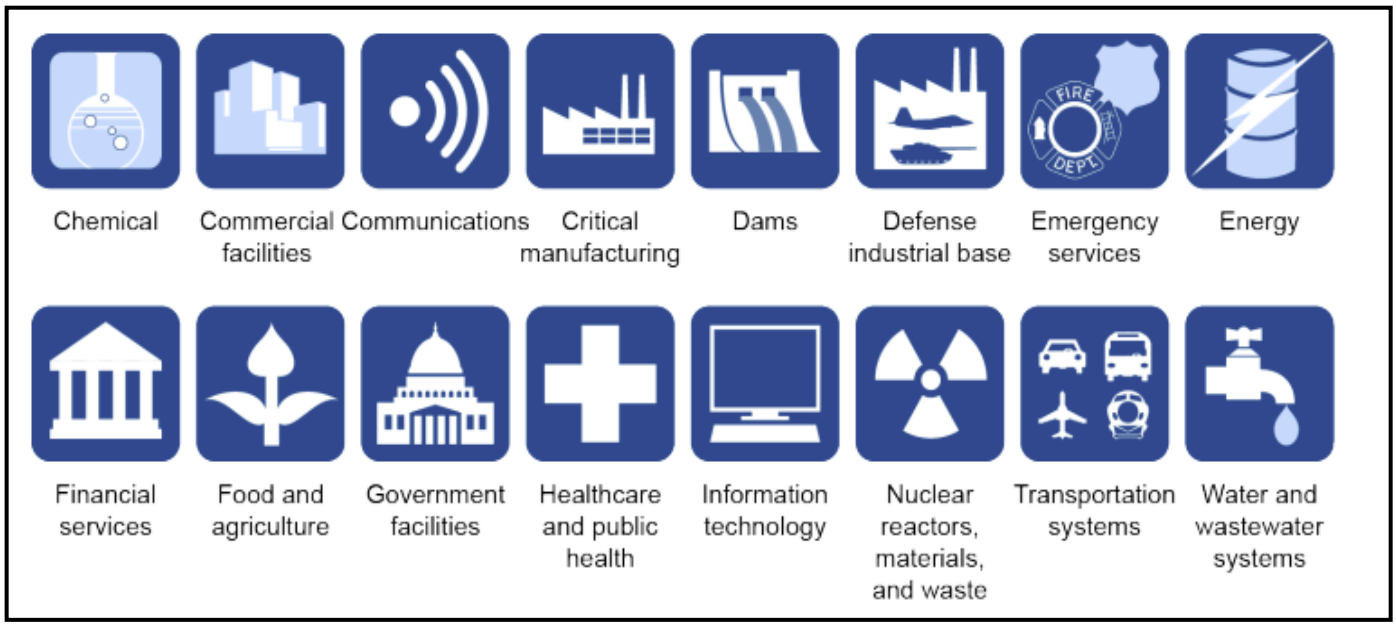
Other Damaging Impacts To An Employer From An Insider Threat Incident

- ☐ 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