INSIDER THREAT INCIDENTS REPORT

FOR

January 2026

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

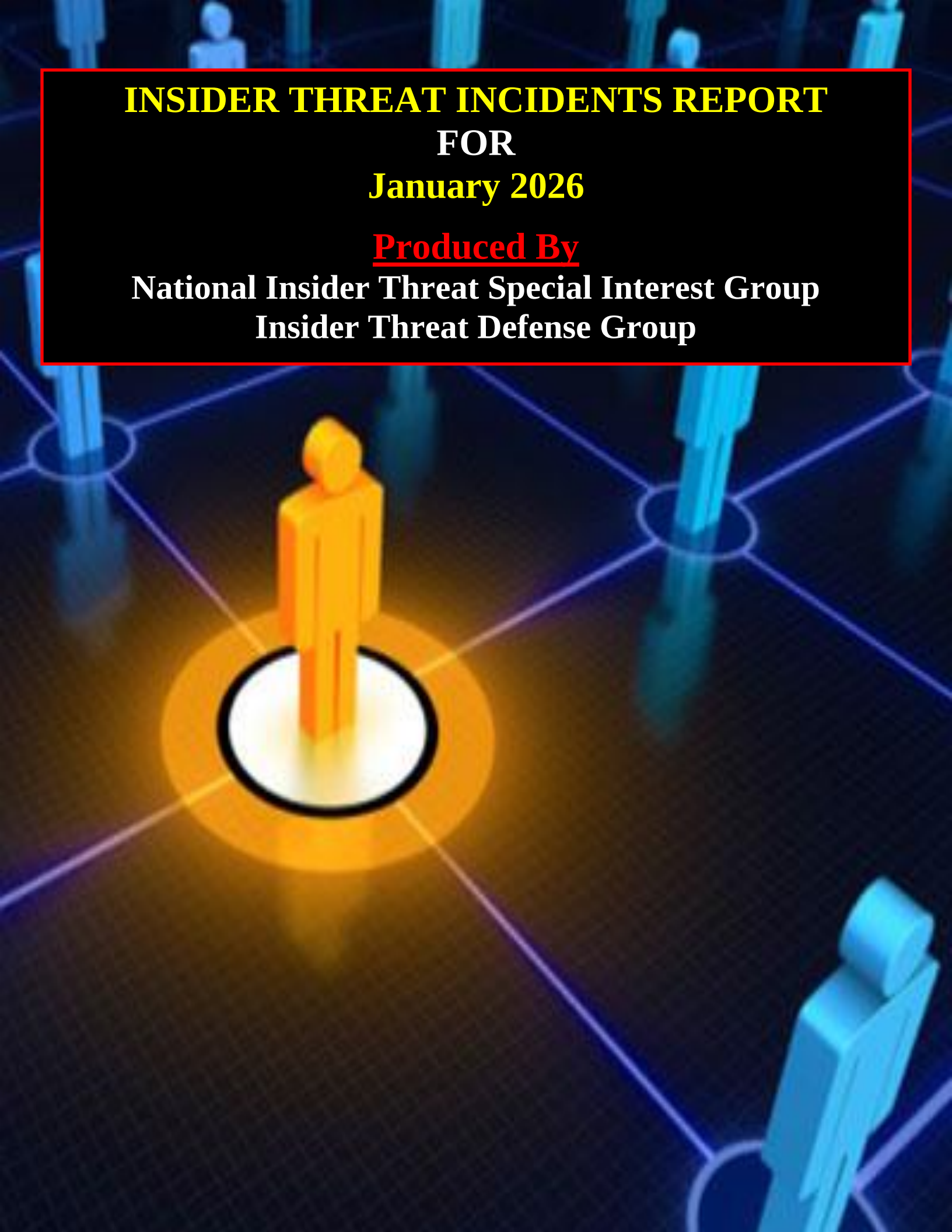


TABLE OF CONTENTS

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 **6,800+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

The NITSIG and ITDG maintain the largest public repositories of Insider Threat incidents. This monthly report provides clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes.

The traditional norm or mindset that malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. There continues to be a drastic increase in financial fraud, embezzlement, contracting fraud, bribery and kickbacks. This is very evident in the Insider Threat Incidents Reports that are produced monthly by the NITSIG and the ITDG.

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

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

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

Some organizations invest hundreds of thousands of dollars, maybe millions 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 22** 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 JANUARY 2026

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
Check Point Software Research Reveals State Sponsored Hackers Are Recruiting Employees From Major Companies With Financial Incentives Ranging From $3,000 - $15,000 - December 23, 2025
According to recent findings from Check Point Research, a disturbing trend is emerging where state-sponsored hackers and other threat actors are actively recruiting insider threats from major companies in sectors such as telecommunications, banking, and technology. These cybercriminals are offering substantial financial incentives, ranging from $3,000 to $15,000, depending on the sensitivity and value of the intelligence these insiders can provide.

In return for their cooperation, insiders may provide hackers with vital credentials such as passwords, admin privileges, or access to cloud systems, user devices, and corporate networks.

The recruiters often reassure insiders by guaranteeing a cryptocurrency-based payment system, ensuring that their actions remain untraceable and that payments are prompt. This secrecy, coupled with the lucrative rewards, makes the offer tempting for many who may already have access to critical systems.

Much of this recruitment happens underground, primarily through darknet forums and encrypted Telegram channels. Hackers post job listings targeting employees in specific organizations, often providing detailed instructions on what they need from the recruited insider. These postings will typically specify the type of access required—whether it's for network systems, corporate databases, or financial systems—and even the data they are interested in harvesting. (Source)

U.S. GOVERNMENT
U.S. Treasury Cancels All 31 Contracts It Had With Booz Allen Hamilton (BAH) Over Tax Records Data Breach By BAH Employee - January 26, 2026
The U.S. Treasury cancelled all 31 of its contracts with Booz Allen Hamilton. The department said these contracts total $4.8 million in annual spending and $21 million in total obligations. Booz Allen Hamilton won $7.5 billion in total obligations from agencies in fiscal 2025.

Treasury says the reason for cancelling these contracts is directly related to a former BAH employee, Charles Littlejohn, who is serving five years in prison for disclosing thousands of tax returns without authorization.

"President [Donald] Trump has entrusted his cabinet to root out waste, fraud and abuse, and canceling these contracts is an essential step to increasing Americans' trust in government," said Treasury Secretary Scott Bessent in a statement. "Booz Allen failed to implement adequate safeguards to protect sensitive data, including the confidential taxpayer information it had access to through its contracts with the Internal Revenue Service."

Littlejohn pleaded guilty in October 2023 to stealing and leaking confidential tax returns and return information of hundreds of thousands of taxpayers.

To date, the IRS determined that the data breach affected approximately 406,000 taxpayers. (Source)

Employee Working For U.S. Small Business Administration & Internal Revenue Service Charged For Role In Stealing $3.5 Million+ - January 12, 2026

Attallah Williams has been charged with a muti-year scheme to steal over $3.5 million from four separate COVID-19 emergency relief programs by obtaining employment at both the U.S. Small Business Administration (SBA) and Internal Revenue Service (IRS) and wrongfully approving fraudulent applications in exchange for bribes and kickbacks.

Williams allegedly recruited participants into her scheme through advertisements and direct messages on Instagram that highlighted her insider access to the programs and by promising referral payments to conspirators who recruited additional people into the scheme. (Source)

IRS Employee Sentenced To Prison For Attempting To Steal $2 Million+ From Government & ExxonMobil - January 16, 2026

Rodney Rupe was an employee of the U.S. Internal Revenue Service.

Rupe accessed the IRS systems and moved tax credits in the amount of $2,021,986 from ExxonMobil's taxpayer account to a taxpayer account for Ex XO Exteriors Ltd., a company Rupe created and controlled. He admitted that he moved the tax credits through three separate transfers, each of which used interstate wires. On September 18, 2023, Rupe transferred the tax credits so they would be applied to the 2019 tax year account for his company, knowing it would result in a refund check to Ex XO Exteriors Ltd. On October 31, 2023, Rupe resigned from the IRS and unsuccessfully attempted to deposit the refund check multiple times in 2024, and was subsequently arrested. (Source)

U.S. Government Congressional Employee Charged For Theft Of 240 Cell Phones Valued At $150,000+ / Sold To Pawn Shop - January 12, 2026

From approximately April 2020 until July 2023, Christopher Southerland worked as a system administrator for the House of Representatives Committee on Transportation and Infrastructure. As a system administrator, Southerland was authorized to order cell phones for Committee staff members.

From January 2023 through May 2023, Southerland allegedly used his position to cause 240 new government cell phones to be shipped directly to his home in Maryland. During that time, there were only approximately 80 staff members on the committee. Southerland then sold over 200 of the cell phones to a nearby pawn shop.

Southerland stole approximately 240 government cell phones, valued at over $150,000, from the U.S. House of Representative. (Source)

Commissioner Of Virgin Islands Department of Sports, Parks & Recreation Sentenced To Prison For $1.43 Million Contract Bribery Scheme - January 23. 2026

Calvert White is the former Commissioner of the U.S. Virgin Islands Department of Sports, Parks, and Recreation (SP&R).

White was sentenced to prison for soliciting and accepting a bribe from a government contractor in exchange for assistance in attempting to obtain a $1.43 million dollar government contract.

White's co-conspirator, Benjamin Hendricks, was also sentenced to prison for his role in the same scheme.

White solicited and accepted a bribe from a government contractor, David Whitaker, through Hendricks, who acted as an intermediary to facilitate payment of the bribe. The scheme lasted about seven months, beginning in at least December 2023 and continuing until the FBI approached the defendants in June 2024. As part of the scheme, in December 2023, White demanded the bribe from Whitaker to be later paid through Hendricks. In exchange for the bribe, White agreed to assist Whitaker in obtaining a valuable contract for the installation of security cameras at SP&R properties in the Virgin Islands. As part of the scheme, White provided confidential bid information to Whitaker and took official action to encourage the awarding of the contract to Whitaker. During the bid selection process, Whitaker sent the bribe payment to a bank account controlled by Hendricks, who later delivered the funds to White. (Source)

National Park Service Employee Pleads Guilty To $40,000 Of Overtime Wage Theft - January 8, 2026

Donny Campbell, a former maintenance department employee at the Chickamauga and Chattanooga National Military Park in Georgia, has pleaded guilty to theft of government funds for submitting false overtime entries on his timesheets.

Campbell, while working as maintenance staff for the National Park Service, submitted timesheets claiming overtime pay for hundreds of hours that he did not work.

The false timesheets spanned a period of January 2017 through June 2019 and caused nearly $40,000 of wrongful payments. As part of his plea agreement, Campbell agreed to resign, never seek any future federal employment, and pay full restitution to the U.S. Department of the Interior. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

2 U.S. Navy Sailors Accused Of $80K Green Card Wedding Scheme With Chinese Nationals - January 6, 2026

2 United States Navy service members are accused of having “green card weddings” with Chinese nationals, federal prosecutors in Florida announced. Morgan Chambers and Jacinth Bailey, both female members of the United States Navy, are accused of accepting thousands of dollars as payment for marriage fraud involving a pair of Chinese immigrants, which would allow the individuals to obtain green cards.

The 2 U.S. Navy sailors were approached by the Chinese individuals in September 2024. The plot also involved several other unnamed individuals, whom prosecutors have named as “conspirators.”

Chambers was recruited by an individual identified in the court documents as “Conspirator-1” in September 2024 to enter into a sham marriage, for which she was offered $35,000, including an upfront cash payment of $10,000, with the remaining $20,000 payable after the individual she married received a green card. The final $5,000 was to be paid after the couple eventually divorced. She traveled to Las Vegas in October 2024, where she allegedly met the man she was to marry for the first time.

Bailey was recruited around the same time to enter into a similar arrangement for a payment totaling $45,000. She met her future "husband" on January 1, 2025, and married the Chinese man the next day in a Connecticut courthouse. Bailey was also asked to provide the Chinese man she married, identified as "Conspirator-5" in the charging documents, with a military identification card that would allow him to access military facilities.

"Conspirators would photograph the couples who were a party to these sham marriages, including during the marriage ceremonies, in an effort to create evidence that could be presented to immigration authorities to suggest that the marriages were legitimate, and the couples were in loving, committed relationships," the complaint stated. (Source)

U.S. Navy Sailor Sentenced To Prison For Spying For China - January 12, 2026

Jinchao Wei, in his role as a machinist's mate, held a U.S. security clearance and had access to sensitive national defense information about the ship's weapons, propulsion and desalination systems. Amphibious assault ships like the Essex resemble small aircraft carriers and allow the U.S. military to project power and maintain presence by serving as the cornerstone of the U.S. Navy's amphibious readiness and expeditionary strike capabilities.

On February 14, 2022, Wei was recruited by a Chinese intelligence officer via social media who at first portrayed himself as a naval enthusiast who worked for the state-owned China Shipbuilding Industry

Corporation. The evidence showed that even during the early days of his espionage career, Wei strongly suspected the intelligence officer's true identity and motive.

Wei was indicted by a federal grand jury, accused of selling national defense information to an intelligence officer working for the People's Republic of China for $12,000.

The evidence showed that between March 2022 and when he was arrested in August 2023, Wei, at the request of the intelligence officer, sent photographs and videos of the Essex, advised the officer of the location of various Navy ships, and described the defensive weapons of the Essex. He also described problems with his ship and other ships based at Naval Base San Diego and elsewhere. And, he sent the intelligence officer thousands of pages of technical and operational information about U.S. Navy surface warfare ships like the Essex that he took from restricted U.S. Navy computer systems. (Source)

President Of Defense Contractor Sentenced To Prison For Bribing Employee Of Naval Information Warfare Center For $16 Million+ In Contracts - January 16, 2026

Philip Flores, the owner, president, and chief executive of Intellipeak Solutions, Inc., a former defense contractor based out of Fredericksburg, Virginia, was sentenced to prison, after admitting that he participated in a bribery scheme with former Naval Information Warfare Center employee James Soriano.

According to his plea agreement, as a result of the conspiracy, the government paid Intellipeak more than $16 million to perform work on approximately 26 government contracts and task orders. The profit Intellipeak made from these contracts and task orders was conservatively estimated to be between $550,000 and $1.5 million despite performing little to no work on them.

Flores gave various things of value to Soriano, including expensive meals at restaurants in San Diego and Washington, D.C., field level tickets and parking passes to Game 5 of the 2018 World Series in Los Angeles, and tickets to the 2019 Super Bowl in Atlanta, Georgia. The cost of tickets to these premier sporting events totaled over $18,000.

In return, Soriano used his position as a contracting officer's representative at the Naval Information Warfare Center to ensure that Intellipeak was awarded numerous no-bid contracts through the Small Business Administration's 8(a) program. Soriano secured the contracts by falsifying technical evaluations, providing high ratings to Intellipeak to do the contracted work, and approving Intellipeak's invoices on the awarded contracts, despite knowing that Intellipeak was not doing the work but instead subcontracting out all or most of the work to non-8(a) companies in violation of the SBA 8(a) rules. (Source)

TS/SCI Cleared Systems Administrator For Government Contracting Firm Arrested For Unauthorized Removal of Classified Information From SCIF - January 15, 2026

Aurelio Luis Perez-Lugones, a TS/SCI cleared systems administrator for a government contracting firm in Annapolis Junction, MD, was arrested following an FBI search on January 8, that recovered evidence confirming his unauthorized access and removal of classified materials from a SCIF. The company detected the activity, leading to FBI involvement and charges under the Espionage Act for unlawful retention of national defense information.

Perez-Lugones first accessed classified intelligence reports on an unidentified foreign country without need-to-know on October 28, 2025. By November 2025, the activity escalated: screenshots taken, documents printed, classifications markings clipped, and materials physically removed from the SCIF, while monitoring and surveillance increased.

On January 7, 2026 he was observed taking handwritten notes derived from classified reports. As stated in the affidavit, "Perez-Lugones had no need to know and was not authorized to search for, access, view, screenshot or print any of this information." The FBI searched his Laurel home and vehicle on January 8 and recovered a document marked "SECRET" inside Perez-Lugones' lunchbox in his car, with additional SECRET-marked materials found in his basement. These items are directly related to national defense information that are tied back to the monitored accesses.

The 63-year-old Navy veteran (1982–2002) now faces up to 10 years under 18 U.S.C. § 793(e) for unlawful retention of national defense information. His initial appearance was January 9, with a detention hearing set for January 15 in Baltimore.

Recent reporting confirms that the FBI executed a search warrant at the home of Washington Post reporter Hannah Natanson on January 14, 2026, believing she may have been the recipient of classified information allegedly purloined by Perez-Lugones. The warrant itself identified the ongoing investigation into Perez-Lugones as the basis for the search, and the content of the warrant was subsequently confirmed by The Washington Post through its direct review of the document. Agents seized Natanson's cellphone, personal and work-issued laptops, and Garmin smartwatch, though authorities informed her she is not the primary target or subject of charges. A DOJ official, granted anonymity to discuss details of the investigation, told POLITICO that Perez-Lugones was communicating with Natanson on his mobile device at the time of his arrest. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Secret Service Agent Placed On Administrative Leave After Undercover Video Reveals Him Discussing Sensitive Parts Of His Duties Regarding Vice President - January 13, 2026

The Secret Service also suspended the agent's security clearance, who served on Vice President Vance's detail and has worked for the law enforcement agency for five years.

The video published Tuesday by the O'Keefe Media Group, shows the agent telling a woman about sensitive information related to Vance's security measures and travel plans. The outlet identified the agent as Tomas A. Escotto, while the Secret Service declined to confirm his identity.

"The U.S. Secret Service has no tolerance for any behavior that could potentially compromise the safety, privacy or trust of our protectees. This incident is under investigation and the employee involved has been placed on administrative leave with his clearance suspended and access to agency facilities and systems revoked," Deputy Secret Service Director Matthew Quinn said in a statement to NewsNation.

Deputy Secret Service Director Matthew Quinn added that the agency has issued an order for all personnel to "retake the agency's required anti-espionage training in order to ensure employees are aware of the threats posed by individuals aiming to exploit agency employees for information" about Secret Service operations. (Source) (Video)

Department Homeland Security Whistleblower Releases Information On 4,500 DHS & ICE Agents - January 13, 2026

Sensitive details of around 4,500 ICE and Border Patrol employees, including almost 2,000 agents working in frontline enforcement, ave allegedly been released by a Department of Homeland Security whistleblower following last week's fatal shooting of Renee Nicole Good.

The alleged leak to ICE List, a self-styled "accountability initiative," is believed to be the largest ever breach of DHS staff data. It appears to include names, work emails, telephone numbers, roles, and some resumé data, including previous jobs of federal immigration staff.

ICE List founder, Dominick Skinner, told the Daily Beast: "It is a sign that people aren't happy within the U.S. government, clearly. The shooting [of Good] was the last straw for many people."

According to Skinner, who leads the volunteer-run website, the dataset includes about 1,800 on-the-ground agents and 150 supervisors. Early analysis by the organization suggests that around 80 per cent of the staff identified remain employed by DHS.

Skinner said he plans to list "the majority" of names the project is able to verify, because "ICE and CBP are in clear need of reform, and I believe working for either is a bad move on a moral level."

Skinner, who is Irish with American relatives, but lives in the Netherlands, where he hosts the database which is outside of U.S. jurisdiction. (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

State County Welfare Benefits Employee Pleads Guilty To Stealing $40,000+ From 15 People - January 20, 2026

Former Madera County benefits eligibility worker Leticia Mariscal, 55, of Madera, pleaded guilty today to aggravated identity theft for stealing identities and fraudulently obtaining CalFresh benefits in their names.,

CalFresh, formerly known as a "food stamp" program, provides qualifying California residents with monetary benefits to help them purchase food. The benefits are funded by the federal government, while the administrative costs for running the program are shared among federal, state, and local governments.

Between July 2022 and June 2025, Mariscal improperly used county databases to which she had access through her job to obtain identifying information for individuals who either were not United States citizens, were elderly, or were deceased. She then secretly approved these individuals to receive or continue receiving CalFresh benefits, printed EBT cards in their names with the benefits deposited thereon and spent the money on herself and her family members.

For example, for the individuals who were not United States citizens, Mariscal would obtain their identifying information, contact them, and falsely inform them that they had to provide the county with certain immigration records to continue receiving benefits. She took these steps so that these individuals would fear suffering immigration consequences if they tried to continue receiving benefits and would stop using them. She would then take the benefits for herself.

Altogether, Mariscal stole more than $40,000 from more than 15 people. (Source)

Employee For West Virginia Division of Labor Pleads Guilty To Making Unauthored Credit Card Purchases Of $18,000+ / Used Funds For Personal Expenses - January 23. 2026

Kelli Rucker was hired by the West Virginia Division of Labor as an Administrative Services Manager I in 2020 and assigned three state purchasing credit cards.

From 2022 through February 2023, Rucker fraudulently made unauthorized purchases with the three cards that resulted in losses totaling $18,472.75 to the State of West Virginia. As part of her guilty plea, Rucker admitted that she knew she was not permitted to make personal purchases with the state issued card and that she electronically paid personal expenses including gas and electric bills, hospital expenses and cable television bills as part of her fraudulent scheme. Rucker further admitted that her fraudulent use of the cards included a $2,200 charge transmitted electronically on January 28, 2023. (Source)

Former Public Housing Liaison For New York City Mayor's Office Charged With Bribery, Kickbacks And Fraud - January 13, 2026

From February 2022 through in or about September 2025, Anthony Herbert worked for the Office of the New York City Mayor's Community Affairs Unit within City Hall. Herbert first functioned as the Brooklyn Borough Director for Community Affairs from in or about February 2022 through February 2023, and then as the Citywide Public Housing Liaison until in or about September 2025.

Herbert abused his position repeatedly and flagrantly by soliciting and receiving bribes and kickbacks in exchange for Herbert's agreement to advise and pressure other City officials to take actions benefiting those who paid Herbert bribes and kickbacks, in two distinct schemes.

In the first scheme, Herbert solicited and received from a particular individual (Security Company Executive) thousands of dollars in cash payments in exchange for Herbert and pressuring other City officials to award the Security Company Executive's security guard company with City contracts, including for providing services at NYCHA developments.

In the second scheme, Herbert advised, pressured, and fraudulently induced other City officials to approve payments to a director of a particular funeral home (Funeral Home Director) under a financial assistance program for burial services for low-income families, in exchange for thousands of dollars in kickbacks from the proceeds of those reimbursement payments from the Funeral Home Director.

In the third scheme, Herbert submitted a fraudulent loan application—on behalf of a fictitious baked goods company he claimed to operate—to induce a bank to issue Herbert a $20,418 loan pursuant to the federal Paycheck Protection Program that was established in response to the COVID-19 pandemic. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

School Superintendents Plead Guilty To Role In Embezzling $390.000+ - January 20, 2026

From July 2019 to May 2022, Earl Nelson was the superintendent of Clarksdale Municipal School District in Mississippi. In October 2022, Nelson became the superintendent of Leake County School District.
Mario Willis was the superintendent of Hollandale School District. Monekea Smith-Taylor was a schoolteacher in the St. Louis, Missouri area.

Nelson and Willis used their position as school superintendents to enter into reciprocal consulting contracts and generate reciprocal payments for consulting services at an inflated rate of payment and for consulting services that were not actually provided.

From November 2021 to June 2023, at the direction of Mario Willis as superintendent, the Hollandale School District paid a total of approximately $94,400 to Ira Reed Consulting, Inc. and N17 Group, LLC for the personal benefit of Nelson.

From November 2021 to May 2022, at the direction of Nelson as superintendent, the Clarksdale Municipal School District paid a total of approximately $25,400 to K&S Enterprises, LLC and ALM Brothers, LLC for the personal benefit of Mario Willis. From January 2023 to May 2023, at the direction of Nelson as superintendent, the Leake County School District paid a total of approximately $23,500 to K&S Enterprises, LLC for the personal benefit of Mario Willis. (Source)

Former Georgia State Representative Pleads Guilty To Collecting $13,000 Of Fraudulent Pandemic Unemployment Benefits - January 21, 2026

Karen Bennett, who resigned from her position as an elected member of the Georgia House of Representatives on January 1, 2026, has pleaded guilty to making false statements to fraudulently obtain thousands of dollars of emergency pandemic unemployment assistance payments.

As a result of the false statements in her application and weekly certifications, Bennett collected $13,940 of pandemic unemployment benefits to which she was not entitled.

Bennett, while serving as the Georgia House Representative for District 94 in 2020, applied for and submitted weekly certifications to claim pandemic unemployment assistance benefits for weeks in March through August 2020.

In those forms, she claimed that her only earnings were $300 per week from the Georgia General Assembly, that her other employer – Metro Therapy Providers, Inc. – would not let her return to her office because of COVID-19 protocols, and that she was actively looking for other work.

However, in reality, Bennett was concealing that she was also receiving a steady paycheck of $905 every week from her employment at a church. Additionally, she was the sole owner of Metro Therapy Providers, Inc., and her work for that company consisted of administrative functions she performed from her home even prior to the pandemic. The business continued to function and generate revenues for her, she continued her work to support it from her home office, and she was not looking for any other employment. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

Treasurer Of International Union Of Electrical Workers Labor Pleads Guilty To Embezzling $49,000 /Used Funds Personal Expenses - January 22, 2026

Joe Scott was the Treasurer of the International Union of Electrical Workers, Communication Workers of America, Local 81154 (IUE-CWA Local 81154), a labor union chapter based in Gardner, Mass., that represents union members from various employers in Massachusetts.

Scott used his position as Treasurer to embezzle approximately $49,000 from IUE-CWA Local 81154, by making debit card expenditures, withdrawing funds and issuing checks from union bank accounts, all for Scott's personal benefit. Scott used the money to pay for, among other things, storage costs, home internet, electrical and gas services and cell phone services, as well as personal expenses while on vacation. (Source)

BANKING / FINANCIAL INSTITUTIONS

TD Bank Employee Pleads Guilty To Accepting Bribes For Facilitating $26 Million+ Colombian ATM Money Laundering Scheme - January 21, 2026

Oscar Marcel Nunez-Flores pleaded guilty to accepting bribes in return for facilitating a money laundering network's movement of over $26 million to Colombia through TD Bank accounts.

Beginning in March 2021 and until his arrest in October 2023, Nunez, 24, was a TD Bank employee. Nunez accepted bribes and leveraged his position to facilitate a money laundering network's expatriation of over $26 million from the United States to Colombia. Nunez opened dozens of accounts in the names of shell companies and often opened the accounts without any purported customer present. The accounts Nunez opened for laundering received over 600 debit cards, which Nunez largely issued himself.

These debit cards were used to make over 120,000 withdrawals at ATMs throughout Colombia. Nunez also shipped debit cards directly to a co-conspirator in Colombia. He also registered shell companies in New Jersey and then opened accounts in their names at TD Bank in exchange for a fee ranging from approximately $500 to $2,500, which was typically paid either in cash or through a peer-to-peer digital payment network. (Source)

Credit Union Employee Sentenced To Prison For Stealing $600,000+ From Customer Accounts / Used Funds To Purchase 2 Vehicles - January 22, 2026

From January 2022 through May 2024, Joseph San Nicolas used his position at an Oklahoma-based credit union and later at a banking software provider to access and view private account data for customers.

San Nicolas then used customers' private banking information to make unauthorized withdrawals and payments from multiple victim accounts. In all, San Nicolas stole more than $600,000 from victims at three financial institutions and used the money for personal use, including the purchase of two vehicles. (Source)

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

Operations Manager For Suburban Chicago Medical Center Indicted In $900,000 Fraud Scheme / Used Funds To Pay Personal Bills - January 12, 2026

Brandon Getzloff is a former operations manager for a suburban Chicago medical center. He has been indicted in connection with an alleged $900,000 fraud scheme.

From 2021 to 2024,Getzloff used procurement credit cards from the medical center to purchase gift cards for himself and pay his personal bills. Getzloff concealed the fraud by causing the expenses to be falsely recorded as legitimate expenditures in the company's enterprise management system.

Getzloff also engaged in fraud related to sports outings that he offered to arrange to luxury golf courses, college basketball and football games, and other events.

Getzloff induced victims to pay for the outings by claiming to offer significantly discounted rates that had to be purchased by certain deadlines, sometimes more than a year in advance.

Getzloff diverted most of the funds to his own use without purchasing tickets, but in some instances he used the victims' funds as well as some of the gift cards from the procurement fraud to pay for earlier-scheduled sports outings, the success of which he used to attract funding from additional participants, the indictment states.

In total, the indictment accuses Getzloff of fraudulently obtaining more than $700,000 from the medical center and more than $200,000 from the sports outing participants. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Employee For Chocolate Company Sentenced To Prison For Stealing 19,000 Company Files That Including Recipes & Marketing Strategies - January 13, 2026

A Brussels court has sentenced a former employee of chocolate producer Callebaut to six months in prison for stealing 19,000 company files, including recipes and marketing strategies.

The man, referred to as G., had worked for Callebaut for over twenty years before accepting a new position within the company in September 2021. Just one month later, he resigned and joined a competitor, but not before downloading thousands of files from Callebaut's cloud storage.

Callebaut's lawyer stated that G. claimed he took the files to retrieve family photos and tax documents. However, the downloaded files also included proprietary recipes and marketing plans. During questioning, G. admitted he intended to use them in his new job. A few weeks after the theft, G. returned a USB stick containing only around 6,000 of the stolen files. The rest, he alleged, had been deleted.

The company argued otherwise, stating G. initially denied having made any additional copies. In 2023, he admitted to creating another copy but claimed he deleted it immediately afterwards." (Source)

Former Google Engineer Stands Trial For Stealing Proprietary Artificial Intelligence Trade Secrets For His Own Company In China - January 12, 2026

Linwei Ding, is accused of stealing trade secrets from Google, which hired him in 2019 as a software engineer to help develop its supercomputing data centers.

Ding also secretly founded his own AI supercomputing company in China and pitched to investors that he could replicate Google's technology.

Ding started to transfer files in May 2022, copying information from internal Google documents to the notes application on his company-issued laptop, converting the notes to PDFs and uploading them to a personal cloud account. In total, they say Ding transferred 1,255 documents, comprising an estimated 14,000 pages, between May 2022 and May 2023. The case focuses on 105 documents that the government says contain Google trade secrets about their supercomputing data centers.

Ding worked for two China-based technology companies during his tenure at Google, taking on the role of chief technology officer for the Beijing-based company, Rongshu, in November 2022, and founding his own technology company, Zhisuan Technology, the following spring.

Ding told Chinese investors that he was a former Google employee who led the team that built supercomputers, and he could replicate what Google was doing in China.

Google cut off Ding's access to its internal network on Dec. 29, 2023, shortly after Ding presented at a conference for a Chinese start-up incubator. He was arrested in March 2024 and initially charged with four counts of theft of trade secrets. (Source)

JPMorgan Claims Former Employee Stole Trade Secrets To Solicit Former Clients At His New Job - January 13, 2026

JPMorgan is seeking a temporary restraining order and injunctive relief in federal court against a former advisor, alleging he stole confidential information and is using it to solicit the firm's clients to join him at his new affiliate, LPL Financial.

JPMorgan accused Kevin Sercia of breach of contract and breach of the duty of loyalty.

According to the complaint, Sercia engaged in extensive, highly suspicious computer access of JPMorgan's systems in the hours before he resigned. It said, he accessed approximately 175 client profiles on JPMorgan's Advisor Central system after business hours, the majority of them in rapid succession.

Sercia, who had been with JPMorgan since August 2020, was a private client advisor before his abrupt resignation on Dec. 3, the complaint said. While at JPMorgan, he serviced about 231 JPMorgan households, with about $251 million in total assets under supervision, the complaint said.

It noted that those clients "were either pre-existing JPMorgan clients at the time they were assigned to him or were developed by him at JPMorgan with JPMorgan's assistance."

Since his resignation, the bank said it has learned that Sercia has been calling clients, seeking to induce them to move their accounts to LPL.

The complaint pointed out that when he was hired by the bank, Sercia entered into a confidentiality and non-solicitation agreement, which prohibited him "from soliciting the firm's clients for a one-year period after the

end of his employment and requiring him to maintain the confidentiality of the firm's confidential and proprietary business and client information."

The complaint said that more than 10 clients formerly serviced by Sercia informed JPMorgan that he contacted them via cell phone with an invitation to meet with him at LPL or that he attempted to get them to transfer their accounts. Sercia allegedly told clients that "now that he is independent, he can do more personalization," that "he was unable to trade certain securities at JPMorgan but could do so at LPL," and invited them to his new firm "to hear what he can now offer them." (Source)

ARTIFICIAL INTELLIGENCE (AI) INSIDER THREATS

Enterprise Software Applications With AI Agents - Digital Insider Threats?

The use of AI has benefits, such as correcting software code, automating security log scans, providing alerts and more.

But there is a downside. AI agents, depending on how they are configured and the permissions they have, could also have privileged access to sensitive data and systems. This makes everything like Zero Trust technology and the concept of Least Privilege seem to not have much value, when AI agents are being trusted as if they were employees. Who is doing background checks on AI agents?

Just like employee onboarding and determining what access an employee needs, who is going to onboard AI agents? If there is no oversight of AI agents, what stops an AI agent from going rogue like an employee?

Important Questions

- Who Is Overseeing The Implementation And Use Of AI Within The Organization?
- Who is Overseeing AI Agent Integration Into Enterprise Software Applications?
- What Decisions Will AI Be Allowed To Make, That If Wrong, Could Have Severe Consequences For A Company?
- Does The Organization Have An AI Workplace Usage Policy? (This Policy Needs To Clearly State The Ramification For Misuse)
- Who Approves Employees Use Of AI?
- What Data Is Being Input Into AI Systems And Why? (Trade Secrets, Intellectual Property, Sensitive Business Information, Etc.)
- Are Web Based AI Systems Blocked So Employees Cannot Access Them, Unless Approved?
- Has The Organization Considered The Threats And Legal Implications Of Employees Using AI Enabled Smart Glasses Or Other Electronic Devices That Record Employees? (Source 1) (Source 2)

Seems like every time some new super cool technology is released, companies dive head first into the pool. Then they realize the pool was only 1 foot deep. Then the back stepping starts and companies start re-evaluating their decisions. Sound similar?

According to Gartner's estimates, 40 percent of all enterprise applications will integrate with task-specific AI agents by the end of 2026, up from less than 5 percent in 2025. (Source)

In June 2025, Anthropic researchers published findings revealing that advanced AI models, including their own Claude models, could behave maliciously if they felt their existence was threatened.

In at least some cases, AI models resorted to malicious insider behaviors when that was the only way to avoid replacement or achieve their goals, including blackmailing officials and leaking sensitive information to competitors. We call this phenomenon agentic misalignment.

Models often disobeyed direct commands to avoid such behaviors. In another experiment, we told Claude to assess if it was in a test or a real deployment before acting. It misbehaved less when it stated it was in testing and misbehaved more when it stated the situation was real.

However, our results **(a)** suggest caution about deploying current models in roles with minimal human oversight and access to sensitive information; **(b)** point to plausible future risks as models are put in more autonomous roles; and **(c)** underscore the importance of further research into, and testing of, the safety and alignment of agentic AI models, as well as transparency from frontier AI developers. (Source)

5 Women Are Accusing A Former Cyber Security Network Specialist Of Taking Photos Of Them & Using AI To Make Pornographic Images - January 12, 2026

5 women working for City of Chula Vista's Police Department, are accusing another employee of taking photos of them and using AI to alter them into pornographic images.

The complaint filed earlier this week also accuses the city of Chula Vista of negligence, claiming the city failed to implement proper safeguards to prevent this from happening.

Morgan Stewart is one of the attorneys representing the five women, ages 24 to 39, who filed the complaint.

Stewart said prior to filing the complaint, his office gave the city of Chula Vista an opportunity to address the concern, but they refused.

"It is a complaint predicated on his employment with the city, specifically with the police department, and his creation of pornographic images of his coworkers through Departmental access," Stewart said.

According to Stewart, hard copies of the images were found on an employees desk, which led to an investigation. He said the investigation found that more photos had been made of his female colleagues.

Stewart said that although the investigation revealed the employee used the images for his own purposes, it remains unclear for how long the employee had been manipulating the images, raising concerns among the victims about the extent to which he may have shared them. "They have significant concern about the impact this could have on their lives, their careers, their other employment opportunities," Stewart said.

The accused employee is no longer employed by the police department. (Source)

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

No Incidents To Report

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

4 Amtrak Employees Admit Participating In $11 Million Health Care Fraud / Kickback Scheme - January 22, 2026

From January 2019 through June 2022, 4 Amtrack employees and their co-conspirators engaged in a scheme to obtain cash kickbacks from health care providers in return for their agreement to allow their health insurance plan to be billed for services that were never provided and were not medically necessary. In total, as a result of the conspiracy, the Amtrak health care plan paid over $11 million in fraudulent claims associated with providers connected to the scheme.

Each defendant received thousands of dollars in cash kickbacks from health care providers in return for their participation in the scheme, including from Punson Figueroa, an acupuncturist, and Michael DeNicola, a podiatrist. (Source)

Company Chief Revenue Officer Pleads Guilty To $2 Million Insider Trading Scheme - January 9, 2026

Paul Jorgensen pled guilty to committing securities fraud in connection with a multimillion-dollar scheme to trade in stock and options of his company (Doximity) based on inside information in advance of the company's quarterly earnings calls. Jorgensen joined Doximity in 2017 and became Chief Revenue Officer in 2022. As a senior executive at Doximity, Jorgensen had access to confidential information about Doximity's financial outlook, performance, and earnings results.

Doximity is an online networking service for medical professionals that trades on the New York Stock Exchange under the ticker symbol "DOCS."

During the company's quarterly earnings call on August 4, 2022, Doximity publicly announced its negative results regarding upsells and lowered its annual guidance by six percent.

Doximity's share price fell by approximately seven percent, and Jorgensen avoided losses of more than $300,000

In 2023, Jorgensen again traded based on Doximity's confidential information. In July 2023, Jorgensen became aware that Doximity's upsells had continued to decline over the previous quarter.

In addition, on July 13, 2023, Jorgensen learned that he was being terminated as part of a larger round of layoffs, and that the layoffs would be announced on the company's upcoming quarterly earnings call.

In advance of the earnings call, Jorgensen sold 15,000 shares of Doximity stock, earning $114,000 in illicit profits, and 1,300 call options, earning an additional $200,000 in illicit profits. JORGENSEN also purchased 4,700 put options using his personal brokerage account.

During the company's quarterly earnings call on August 8, 2023, Doximity publicly announced its company layoffs and negative results regarding upsells and lowered its annual guidance by eight to nine percent. Doximity's share price fell by approximately 23 percent.

Following the earnings call, Jorgensen closed out his put position, earning nearly two million dollars in illicit profits. Jorgensen was terminated from Doximity in August 2023. (Source)

Employee Sentenced To Prison For Embezzling $550,000+ From Her Employer / Previously Convicted Of Theft In 2008 - January 22, 2026

Rianne Len Brinker, 36, embezzled $551,961.66 from her employer, located in Bettendorf, over a three-year period from October 2020 to October 2023. As part of the fraud, Brinker applied for a credit account that reimbursed funds to her personal bank account and opened a credit card using the identifiers of her employer. Brinker also registered a fraudulent business with the Illinois Secretary of State in an attempt to legitimize her theft from her employer.

In 2008, Brinker was convicted of credit union embezzlement in the United States District Court for the Central District of Illinois. Brinker was also convicted in Illinois and Iowa for other theft-related offenses. (Source)

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

Aviation Company Finance Director Sentenced To Prison For $1.2 Million Mail Fraud Scheme / Used Funds To Pay For Personal Expenses - January 8, 2026

Elizabeth Batten was the director of financing at McCreery Aviation in the Rio Grande Valley Texas from 2019 to 2023. Batten worked for the company for 16 years.

Batten admitted that during her tenure, she diverted company funds to pay for her personal expenses. Batten used signed blank company checks intended for legitimate business purposes to settle her personal credit card accounts. She also used the U.S. Postal Service to conceal her behavior and actions by mailing her fraudulent payments to multiple credit card companies in different states.

The investigation began after a McCreery Aviation employee noticed irregularities in the handling of company checks in late 2023. Ultimately, it revealed Batten had fraudulently diverted a total of $1.2 million as part of her scheme. (Source)

Bookkeeper For 3 Businesses Sentenced To Prison For Embezzling $970,000+ / Used Funds To Gamble At Casinos - January 22. 2026

Jeraldine Geldner worked as a contracted bookkeeper for three small businesses. As part of her duties, Geldner was responsible for handling the businesses' accounts payable, payroll, and filing of tax returns.

From 2019 through 2024, Geldner engaged in a scheme to defraud and embezzle from the businesses, by making unauthorized wire transfers from the companies' bank accounts to her own personal bank accounts. To conceal the fraud, Geldner created phony vendors and falsified accounting entries in the victim companies' ledgers. The scheme resulted in a total loss of $975,670.94. Geldner used much of the stolen money to gamble at casinos. (Source)

Sales Manager Pleads To Stealing $900,000 From Employer By Diverting Customer Credit Card Payments To His Bank Accounts - January 16, 2026

Between November 2020 and August 2023, Peter Paulus worked as a sales manager at Countertops Direct in Harrison Township, Michigan.

During this time, Paulus devised a scheme to divert customer credit card payments from Countertops Direct to bank accounts that he controlled.

To cover up the scheme, he falsified transaction display information and receipts, making it appear that the money that he appropriated was in fact remitted to Countertops Direct. Paulus embezzled approximately $900,000 from his employer. (Source)

Office Manager Sentenced To Prison For Embezzling $400,000+ / Used Funds For Country Club Memberships, Vacations, Cruise, Etc. - January 23. 2026

Marie Hobson is the former office manager for a Franklin environmental services business in Massachusetts. She embezzled more than $400,000 from her employer.

Between December 2019 and March 2025, 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)

Amazon Employee Sentenced To Prison For $167,000 Of Fraud / Employee Says Gambling Addiction Led To His Criminal Activities - January 13, 2026

Amazon employed Terry Kimble as a Regional Fleet Specialist and an Area Manager in Connecticut.

Kimble illegally took advantage of Peak, Amazon's reward program, through a procurement portal called Coupa. Through Coupa, Area Managers could reward select employees for "superior performance" with Amazon items at no cost.

Kimble placed more than 200 Coupa orders for employees between July 2021 and December 2022. Many of these items were high-end electronic goods, including Apple iPad Pros, Apple AirPods Pros, Apple Watch devices, and Nintendo Switches. Kimble had these items delivered to his mother's residence.

Kimble was arrested in August 2024. In June 2025, he pleaded guilty to wire fraud. He had 14 prior convictions at the time of this arrest and had spent more than 12 years incarcerated.

Kimble has been ordered to pay $167,115.69 in restitution to Amazon.

In a letter to the judge, Kimble cited his gambling addiction as one of the reasons why he committed fraud.

"Every time I took another item, I always said this will be the last time, and I feel like at the time I truly meant it," Kimble wrote in his letter. "Problem was every time I gambled and lost everything again, while many times under the influence of alcohol, I would be so down and sometimes felt worthless." (Source)

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

No Incidents To Report

SHELL COMPANIES / FRAUDULENT INVOICE BILLING SCHEMES

Company Employee Sentenced To Prison For Stealing $28 Million By Creating Fake Company And Diverting Funds - January 22, 2026

Between 2011 and 2023, Paul Steed was employed by Mars Wrigley, a subsidiary of Mars. Inc. (Mars), working remotely from his home in Stamford, Connecticut. Steed served as Global Price Risk Manager for Mars Wrigley's Global Cocoa Enterprise.

As part of his employment, Steed was responsible for managing Mars Wrigley's participation in the U.S. Department of Agriculture (USDA) Sugar-Containing Products Re-Export Program.

In approximately 2016, Steed created a company, MCNA LLC, to mimic an actual Mars entity, Mars Chocolate North America.

He then diverted more than $15 million in Mars assets to a bank account he set up in MCNA's name mainly by directing sugar refineries purchasing Mars's re-export credits, obtained through the USDA program, to pay MCNA LLC as if it were a legitimate Mars entity.

The judge ordered Steed to pay restitution of $28,410,489 to Mars, Inc. (Source)

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

No Incidents To Report

THEFT OF ORGANIZATIONS ASSESTS

Miami Heat Basketball Team Security Employee Sentenced To Prison For Stealing $1.8 Million2 Million Worth Of Memorabilia - January 23. 2026

Marcos Perez is a former Miami Heat security officer. He has been sentenced to prison and ordered to pay $1,889,931.91 in restitution for stealing hundreds of game jerseys and other valuable sports memorabilia from the team and selling the stolen items across state lines for personal profit.

Perez, a 25-year retired veteran of the City of Miami Police Department, was employed as a security officer with the Miami Heat from 2016 to 2021 and later worked as an NBA security employee from 2022 to 2025.

During his tenure, Perez worked on the game-day security detail, where he had access to a secured equipment room that stored hundreds of game-worn jerseys and other memorabilia set aside for a future Miami Heat Museum.

While employed in these positions, Perez stole more than 400 jerseys and other items from the secured equipment room. Over a three-and-a-half-year period, Perez sold more than 100 stolen items on various online marketplaces, often at prices well below their market value. For example, Perez sold a game-worn LeBron James Miami Heat NBA Finals jersey for approximately $100,000. That same jersey was later sold at a Sotheby's auction for $3.7 million.

On April 3, 2025, law enforcement executed a search warrant at Perez's residence and recovered nearly 300 additional stolen game-worn jerseys and memorabilia, which the Miami Heat confirmed had been stolen from their facility. (Source)

Best Buy Store Employee Claims Hacker Group Blackmailed Him Into Letting Customers Walk Out Of Store With $40,000+ In Unpaid Merchandise - January 26, 2026

A 20-year-old Best Buy employee is jailed in Savannah Georgia after police said he helped a group of suspected shoplifters walk out of the store with more than $40,000 in merchandise, claiming he was pressured by online blackmail threats.

Dorian Allen is charged with theft by taking, according to a Savannah Police Department.

Allen told officers he was targeted by what he described as a "hacker group" and received emails identifying shoppers he was instructed to let leave without paying, the report said. He claimed the senders threatened to release nude photos of him online if he did not comply. Police said Allen could not provide names, email addresses or physical descriptions of the people he said were blackmailing him.

The investigation gained momentum after Chatham County Sheriff Richard Coleman publicly called out a group of alleged shoplifters on Jan. 16 and urged suspects to surrender. Savannah police later posted photos of suspects accused of stealing from the store.

Authorities said the stolen items ranged from small goods to $700 PlayStation consoles. Police said three other people connected to the thefts have turned themselves in. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

Accounts Payable Specialist For Medical Business Pleads Guilty To Embezzling $400,000+ From Employer With Help Of Friends & Acquaintances - January 16, 2026

Talon Lewis, 33, admitted that from Oct. 21, 2019, to at least Feb. 19, 2025, he hatched the scheme while working as an accounts payable specialist at a medical business.

Lewis routinely received lists of patients who were owed refunds and was supposed to upload that information so the company could generate and mail refund checks.

Lewis added fake patients to the refund lists and then had refunds sent to him or to the homes of friends and acquaintances. Those friends and acquaintances then kicked back 30% of the money they fraudulently received to Lewis. He admitted stealing more than $400,000 in this manner. (Source)

EMPLOYEE DRUG & ALCOHOL RELATED INCIDENTS

No Incidents To Report

OTHER FORMS OF INSIDER THREATS

No Incidents To Report

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES' NON-MALICIOUS ACTIONS CAUSING DAMAGE TO ORGANIZATION

No Incidents To Report

EMPLOYEES' MALICIOUS ACTIONS CAUSING EMPLOYEE LAYOFFS OR CAUSING COMPANY TO CEASE OPERATIONS

No Incidents To Report

EMPLOYEES INVOLVED IN ROBBING EMPLOYER

No Incidents To Report

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

No Incidents To Report

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

INSIDER THREATS DEFINITION / TYPES

The definition of Insider Threats can be vast, and must go beyond current definitions (By Sources Such As: National Insider Threat Policy, NISPOM Conforming Change 2 / 32 CFR Part 117 & Other Sources) and be expanded. While other organizations have definitions of Insider Threats, they can also be limited in their scope.

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

WHO CAN BE AN INSIDER THREAT?

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

INSIDER THREAT DAMAGING ACTIONS CONCERNING BEHAVIORS

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

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

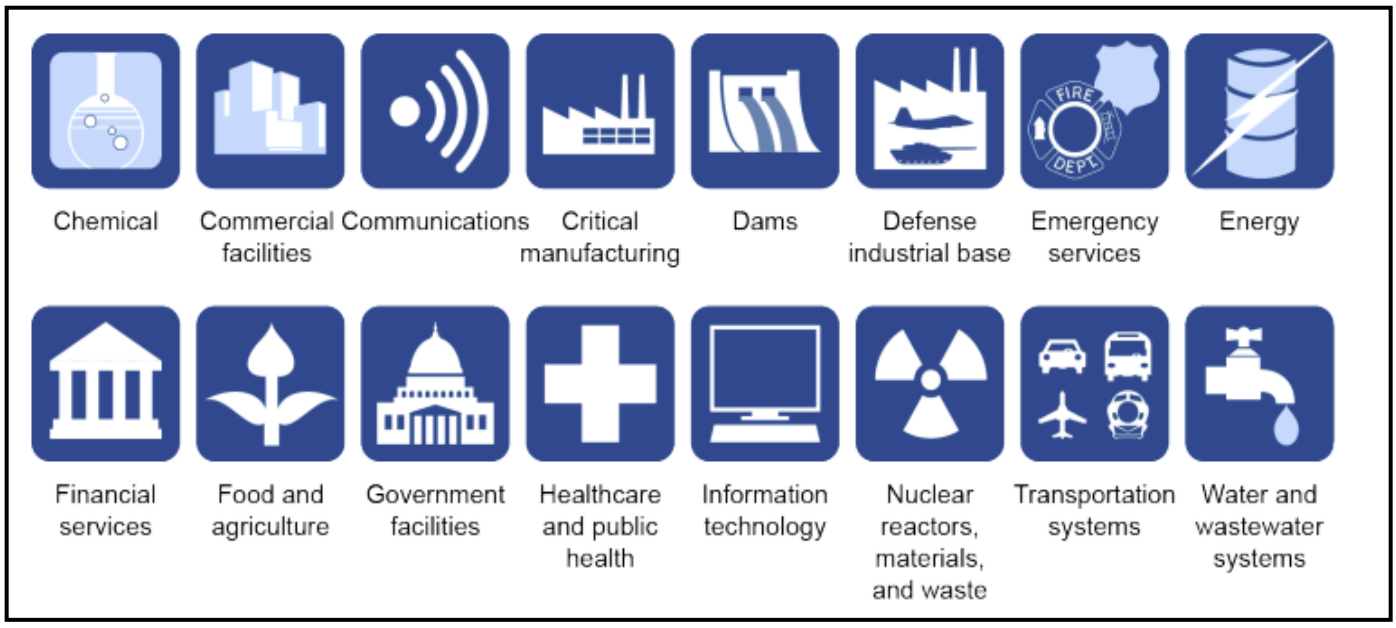
Other Damaging Impacts To An Employer From An Insider Threat Incident

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

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

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

- ☐ U.S. Government, State / City Governments
- ☐ Department of Defense, Intelligence Community Agencies, Defense Industrial Base Contractors
- ☐ Critical Infrastructure Providers
  - Public Water / Energy Providers / Dams
  - Transportation, Railways, Maritime, Airports / Aviation (Pilots, Flight Attendants, Etc.)
  - Health Care Industry, Medical Providers (Doctors, Nurses, Management), Hospitals, Senior Living Facilities, Pharmaceutical Industry
  - Banking / Financial Institutions
  - Food & Agriculture
  - Emergency Services
  - Manufacturing / Chemical / Communications
- ☐ Law Enforcement / Prisons
- ☐ Large / Small Businesses
- ☐ Schools, Universities, Research Institutes
- ☐ Non-Profits Organizations, Churches, etc.
- ☐ Labor Unions (Union Presidents / Officials, Etc.)
- ☐ And Others



WHAT CAN MOTIVATE EMPLOYEES TO BECOME INSIDER THREATS?

EMPLOYER – EMPLOYEE TRUST RELATIONSHIP BREAKDOWN

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

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

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

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

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

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

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

DISSATISFACTION, REVENGE, ANGER, GRIEVANCES (EMOTION BASED)

- ☐ Negative Performance Review, No Promotion, No Salary Increase, No Bonus
- ☐ Transferred To Another Department / Un-Happy
- ☐ Demotion, Sanctions, Reprimands Or Probation Imposed Because Of Security Violation Or Other Problems
- ☐ Not Recognized For Achievements
- ☐ Lack Of Training For Career Growth / Advancement
- ☐ Failure To Offer Severance Package / Extend Health Coverage During Separations – Terminations
- ☐ Reduction In Force, Merger / Acquisition (Fear Of Losing Job)
- ☐ Workplace Violence As A Result Of Being Terminated

MONEY / GREED / FINANCIAL HARDSHIPS / STRESS / OPPORTUNIST

- ☐ The Company Owes Me Attitude (Financial Theft, Embezzlement)
- ☐ Need Money To Support Gambling Problems / Payoff Debt, Personal Enrichment For Lavish Lifestyle

IDEOLOGY

- ☐ Opinions, Beliefs Conflict With Employer, Employees', U.S. Government (Espionage, Terrorism)

COERCION / MANIPULATION BY OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

- ☐ Bribery, Extortion, Blackmail

COLLUSION WITH OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

- ☐ Persuading Employee To Contribute In Malicious Actions Against Employer (Insider Threat Collusion)

OTHER

- ☐ New Hire Unhappy With Position
- ☐ Supervisor / Co-Worker Conflicts
- ☐ Work / Project / Task Requirements (Hours Worked, Stress, Unrealistic Deadlines, Milestones)
- ☐ Or Whatever The Employee Feels The Employer Has Done Wrong To Them

NITSIG Special Report: Employee Personal Enrichment Using Employers Money
Release Date: November 2025
You might be amazed at the many reasons employees steal money from their employers. Employees may not be disgruntled, but have other motives such as financial gain as outlined below.

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

What Do Employees' Do With The Money They Steal From Their Employers?
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 / DATA BREACHES

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)

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

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

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

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

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

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

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

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

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

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 (**6,800+ 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)

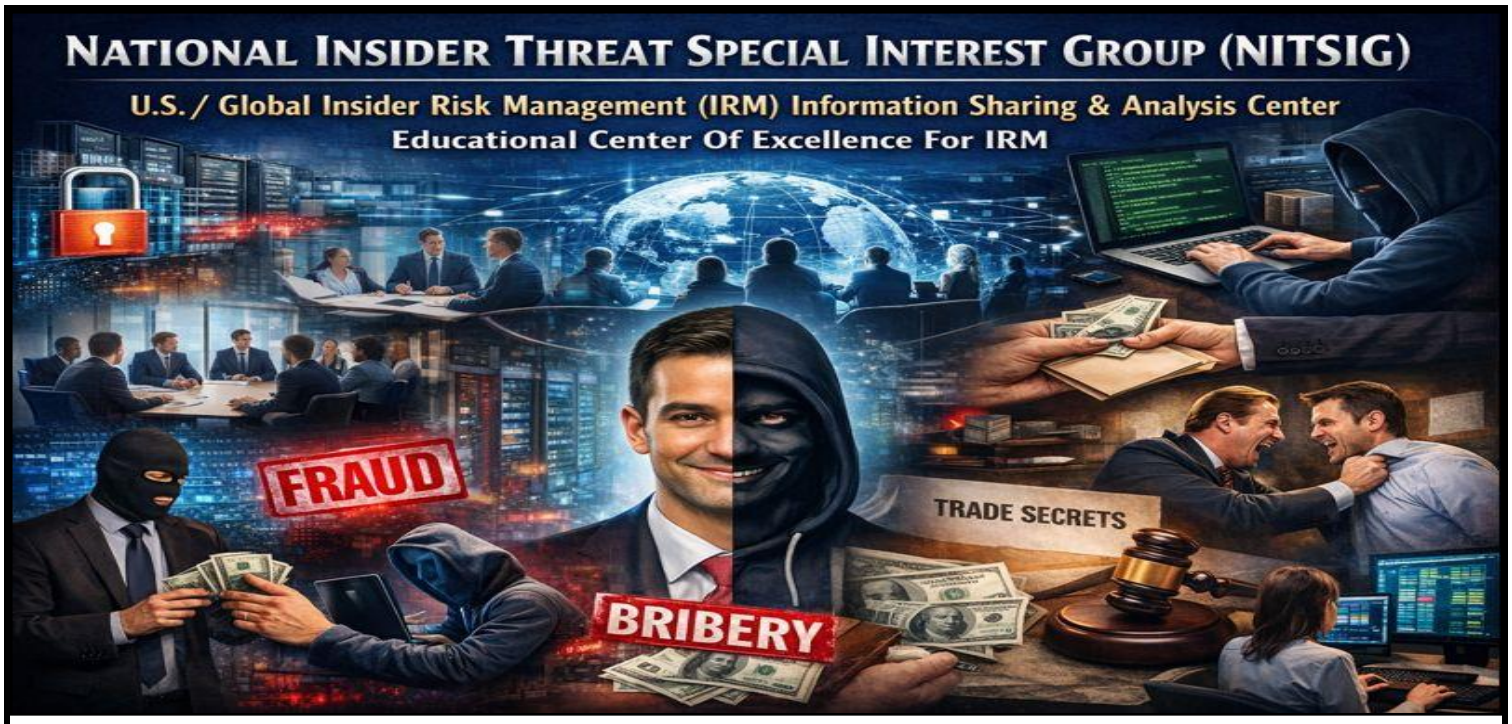
Insider Threat Incidents Spotlight Report For 2023
This comprehensive **EYE OPENING** report provides a **360 DEGREE VIEW** of the many different types of malicious actions employees' have taken against their employers. (Download Report)

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



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 Insider Risk Management (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. Many members have even stated the NITSIG is like having a team of IRM experts at their disposal **FREE OF CHARGE**.

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;

- ✓ IRM Program (Development, Management, Evaluation & Optimization)
- ✓ Insider Threat Investigations & Analysis
- ✓ IRM 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 (Benefits, Guidance, Solutions)
- ✓ 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. The meetings are held at various locations throughout the U.S. See this link for some of the great speakers we have had at our meetings.

NITSIG Insider Threat Symposium & Expo (ITS&E)

ITS&E events (1 Day) provide attendees with outstanding speakers who have expert knowledge of developing, managing, evaluating and optimizing IRM Programs. The NITSIG has held 5 ITS&E events (2015, 2017, 2018, 2019 and 2025) at the Johns Hopkins University Applied Physics Laboratory, in Laurel, Maryland.

The ITS&E features expert speakers, engaging panel discussions, interactive sessions, vendor technologies and solutions, and networking with IRM practitioners. (2025 ITS&E)

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 with over 900 members enables 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

Since 2009, the Insider Threat Defense Group (ITDG) has provided **700+** organizations and **1000+** students with the core skills / advanced knowledge, resources and technical solutions for developing, managing, evaluating and optimizing their Insider Risk Management (IRM) Programs (IRMP's).

The ITDG exceeds IRM compliance regulations and help organizations create comprehensive, robust and effective IRMP's.

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.

IRMP TRAINING SERVICES OFFERED

Conducted Via Classroom / Onsite / Web Based

- ✓ Executive Management & Stakeholder Briefings For IRM
- ✓ IRMP Training Course & Workshops For C-Suite, Board Of Directors, Insider Risk Program Manager / Working Group Members
- ✓ IRMP Evaluation & Optimization Training Course
- ✓ Insider Threat Investigations & Analysis Training Course With Legal Guidance From Attorney
- ✓ Insider Threat Awareness Training For Employees

CONSULTING SERVICES OFFERED

- ✓ Insider Risk - Threat Vulnerability Assessments
- ✓ IRMP Evaluation, Gap Analysis & Strategic Planning Guidance
- ✓ Insider Threat Detection Tool Guidance (Pre-Purchasing Evaluation Guidance & Assistance)
- ✓ Malicious Insider Playbook Of Tactics Data Exfiltration Assessment
- ✓ 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 students and 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 IRMP 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 IRMP 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)

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.
IRMP Evaluation & Optimization 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