INSIDER THREAT INCIDENTS REPORT
FOR
September 2025

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

SPECIAL TRIBUTE TO
Matthew Cheeseman / NITSIG Advisory Board Member

It is with very deep sadness that the NITSIG announce the recent sudden passing of one of our advisory board members, Matthew Cheeseman. His contributions to the monthly reports, the NITSIG mission and his unwavering dedication as an ITP Senior Official for his company will be deeply missed.

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 **6,600+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

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

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

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

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

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

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

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

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

These monthly reports are recognized and used by Insider Risk Program Managers and security professionals working for major corporations, as an educational tool to gain support from CEO's, C-Suite, key stakeholders and supervisors for Insider Risk Management (IRM) Program's. The incidents listed on pages **4 to 26** 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 SEPTEMBER 2025

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

4 Employees And Security Guard Arrested For Stealing $28,000+ Of Fuel From Power Station In South Africa - August 21, 2024

Eskom has confirmed the arrest of four employees and a contractor security guard in connection with the theft of heavy fuel oil, valued at R500 000 (U.S. Dollars $28,831.27) from the Camden Power Station.

The investigation began during a routine quality inspection of coal deliveries at Camden Power Station conducted by Eskom's Security Investigation team.

A suspicious truck attempting to leave the station was intercepted, and the driver was asked to park on the side of the road. Upon presenting a weighbridge slip, the driver claimed that 30 610 kilograms of heavy fuel oil had been offloaded at Camden Power Station. However, a subsequent inspection revealed that the truck was still fully loaded with the fuel oil. The driver fled the scene, triggering further investigations that led to the arrests.

Following further investigations, authorities arrested two more Eskom employees, a weighbridge operator and a control room operator, as well as a contractor security guard. (Source)

GEOPOLITICAL PROBLEMS AND PROTESTS BY EMPLOYEES

Guam Department Of Public Health And Social Services Employee Sentenced To Prison For Stealing $149,000+ - September 2, 2025

Natasha Peredo Vitug was previously employed as an Eligibility Specialist at the Guam Department of Public Health and Social Services (DPHSS). In that role, Vitug was responsible for processing benefits applications, determining eligibility, and issuing benefits.

During the time of her employment, Vitug exploited her position in order to unlawfully re-apply for Cash Assistance Program (CAP) and Supplemental Nutrition Assistance Program (SNAP) benefits in the names of beneficiaries who had left Guam or terminated their participation in the programs. The court ordered Vitug to pay restitution in the amount of $149,944.84. (Source)

U.S. GOVERNMENT

U.S. Postal Service Letter Carrier Sentenced To Prison For Stealing & Selling $10 Million+ Worth of Checks From The Mail - September 8, 2025

From 2020 through August 2024, Rashad Stolden stole mail containing large value checks, as well as debit cards from the California Employment Development Department (EDD), which manages the state's unemployment insurance program.

Stolden worked alongside another letter carrier and friends, Charlie Green. Stolden and Green sold the checks they stole to co-conspirators who then used counterfeit identity documents to negotiate them. Stolden and his co-conspirators purchased the identifying information of victims so that they could activate their stolen EDD cards.

In June 2022, Stolden stole a $7.3 million Treasury check. He then sold the check to a co-conspirator, who negotiated it at a bank in Tennessee, writing him, "I need you man," "I'm trying to retire,". The co-conspirator was able to withdraw more than $1 million from the deposit of this check.

Nowhere in Stolden's voluminous communications throughout this conspiracy did he express any empathy for his victims even as he stole their EDD cards containing their disability and unemployment benefits," prosecutors argued in a sentencing memorandum. Stolden seemed to think only of his own profits, trying to decide whether he should use his thefts to pay for a $13,000 hotel stay in Bora Bora, or if he should upgrade to a $20,000 stay in the Presidential Villa at the Conrad. (Source)

U.S. Postal Worker Stripped Of Citizenship, Sentenced To Prison For Stealing $1.6 Million From U.S. Mail / Used Funds For Lavish Lifestyle, Strip Clubs, Etc. - September 3. 2025

Hachikosela Muchimba, 45, is a former letter carrier for the U.S. Postal Service.

Muchimba was stripped of his U.S. citizenship and to prison today in connection with mail theft and bank fraud scheme that illegally netted him $1.6 million.

Muchimba, originally of the Republic of Zambia, was naturalized as an American citizen on May 26, 2022. The mail theft and bank fraud scheme ran from December 2020 until March 2023. On his application for citizenship he falsely claimed to United States Citizenship and Immigration Services that he had not previously committed any criminal activity, all the while he was actively conducting his theft of mail and scheme to defraud. Because it was unlawfully procured, the Court revoked Muchimba's citizenship.

Between December 2020 and March 2023, Muchimba was a letter carrier based in Friendship Heights, when he executed a scheme to steal U.S. Treasury checks and private party checks from the U.S. mail. The stolen checks were intended for District postal customers living on over 30 different mail routes. Muchimba deposited the checks, sometimes while wearing his U.S. Postal uniform, into bank accounts under his control. Bank surveillance footage captured images of him making deposits and withdrawals of the funds.

The total amount of the U.S. Treasury checks fraudulently deposited into Muchimba's various bank accounts was over $1.6 million. Muchimba used the money to fund a lavish lifestyle that included international travel, stays at luxury hotels, and $100,000 spent at gentlemen's clubs.

The judge ordered Muchimbato to pay $651,068.35 in restitution to victims and to forfeit his ill-gotten gains of $1,273,403.36. Muchimba also will be subject to deportation. (Source)

U.S. Postal Service Employee Pleads Guilty To $278,000+ Of Workers' Compensation Fraud While Employed - September 19, 2025

Sandra Throneburg was employed by the U.S. Postal Service (USPS) as a rural carrier in Valdese, N.C.

On or about September 8, 2015, Throneburg sustained an injury at work while performing her duties. Throneburg stopped working for the USPS because of her injury. On October 23, 2015, she began receiving compensation benefits, in the form of medical benefits and disability compensation administered by the U.S. Department of Labor's (DOL) Office of Workers' Compensation Programs (OWCP) for employees covered by the Federal Employees' Compensation Act (FECA).

In order to receive and maintain FECA benefits, Throneburg was required to report, among other things, all employment, self-employment, involvement in business enterprises, and volunteer work. On or about September 24, 2020, Throneburg completed, signed, and submitted a DOL OWCP Form EN 1032 that contained materially false responses to questions related to her employment status. For example, as Throneburg admitted in court today, she gave negative responses to questions related to whether she had worked for any other employer or was self-employed.

Contrary to statements Throneburg made on the form, between 2016 and 2020, Throneburg had worked for an accounting firm where she performed clerical duties and had received compensation. According to filed court documents, Throneburg failed to disclose to OWCP or USPS that she was employed by and receiving earned income from the accounting firm, while also receiving over $261,000 in workers' compensation benefits, and OWCP had paid over $278,000 for Throneburg's medical bills related to her alleged medical condition. (Source)

U.S. Postal Service Mail Handler Sentenced To Prison For Stealing And Selling $149,000+ Of Checks - September 5, 2025

Vincent Gailliard was employed as a mail handler at the USPS Processing and Distribution Center in Columbia, South Carolina.

The investigation revealed that between April 2022 and May 2023, Gailliard would steal mail containing bank checks that had been mailed by individuals and businesses and take pictures of these checks with his personal cell phone. He would offer to sell an image of the check online that included the account and routing numbers. The buyer could then use the stolen information to create false and fraudulent checks which could be used in obtaining and attempting to obtain money, goods and services. Gailliard was ordered to pay $149,692.14 in restitution. (Source)

U.S. Postal Service Contractor Sentenced To Prison For Stealing $22,000+ Worth Of Checks From Mail - September 5, 2025

Rachel Sanders worked in Franklinton Louisiana as a U.S.Postal Highway Contract Route Contractor.

Sanders stole over forty checks from the mail, forged endorsements on the stolen checks, and deposited them into her own bank account. The losses totaled $22,717.66. (Source)

U.S. Postal Service Mail Carrier Charged For Theft Of Postal Customers' Prescription Drugs - September 5, 2025

Michael Vernon worked as a USPS mail carrier in Waltham, Massachusetts.

From around June 2022 through January 2024, Vernon allegedly used his official position to rifle through the contents of mail entrusted to him, including packages containing prescription medication. It is alleged that Vernon stole bottles of prescription drugs intended for postal customers on his delivery route in Waltham. (Source)

U.S. State Department Employee Sentenced To Prison For Providing Classified Information To Chinese Government Agents For $10,000 Bribe - September 4, 2025

Beginning in April 2022, Michael Schena, 42, communicated with people he met online through various communication platforms and provided them sensitive government information in exchange for money. Two of these individuals represented themselves as employees of international consulting companies. Despite clear indications that they were working on behalf of the PRC, Schena continued his relationship with them.

In August 2024, Schena met an individual at a hotel in Peru who provided Schena $10,000 and a cellphone that was intended to be used for Schena to receive taskings and to image and transmit information.

In October 2024, while at work, Schena photographed and transmitted at least four classified documents that contained national defense information and were classified at the SECRET level.

In February 2025, surveillance video captured Schena again using the cellphone he received in Peru to photograph seven documents marked as SECRET that contained national defense information. FBI agents seized the cellphone before Schena could transmit photographs of these classified documents to his handlers and was later arrested. (Source)

U.S. State Department Budget Analyst Sentenced To Prison For Embezzling $650,000+ / Deposited Money Into Personal Accounts - September 18, 2025

Levita Ferrer admitted that she abused her signature authority over a State Department checking account between March 2022 and April 2024 while working as a Senior Budget Analyst in the State Department's Office of the Chief of Protocol.

Ferrer issued 60 checks payable to herself and three checks payable to another individual with whom she had a personal relationship. She printed and signed each check and then deposited all 63 checks, which totaled $657,347.50, into her personal checking and savings accounts.

Ferrer attempted to conceal her scheme by using a common QuickBooks account at the State Department. After entering her name as the payee on checks in QuickBooks and then printing them, she often changed the listed payee in QuickBooks from herself to an actual State Department vendor. As a result, anyone viewing those entries in the QuickBooks system did not see Ferrer's name as the payee on the checks unless they accessed an audit trail. (Source)

Government Accountability Office Audit Report Reveals Majority Of U.S. Government Agenices Do Not Have A Handle On Their Cyber Security Workforce - September 2025

The vast majority of agencies do not have a handle on their cybersecurity contractor workforce, according to a new report from the Government Accountability Office (GAO) that paints a broader picture of lackluster data collection on federal cyber staffing.

Per the GAO's audit, 22 out of 23 Chief Financial Officers Act agencies reported either partial or no data on the size and costs of their contractor cyber workforce. The review, conducted from February 2024 to September 2025, did not include the Department of Defense.

The Office of Personnel Management was the lone agency that reported to GAO what it believed to be a comprehensive picture of its contractor cyber workforce, while 14 agencies submitted partial data and eight agencies had no data to report at all.

"Generally, agencies attributed their data gaps to either the lack of an agency-wide reporting mechanism or the structure of their contracts," the GAO noted. "Agency officials stated that obtaining data on their contractor cyber workforce required an agency-wide data call or manual review."

As of April 2024, agencies reported employing at least 63,934 federal cyber practitioners plus an additional 4,151 contractor staff, at a cost of approximately $9.3 billion and $5.2 billion, respectively. But the GAO warned that those figures were "incomplete and unreliable and do not reflect the full size and cost of the cyber workforce."

The GAO laid much of the blame for shoddy data quality on the White House's Office of the National Cyber Director, writing that it "has not identified steps that are needed to improve the quality of cyber workforce data used by agency-level" chief human capital officers and chief information officers.

ONCD and the Office of Management and Budget have created working groups to bolster data-informed decision making, the GAO noted, in addition to recognizing "the importance of having quality data on the cyber workforce,"

"Nonetheless, issues remain with respect to data gaps, quality assurance processes, and variances in identifying cyber personnel," according to the watchdog, which found that 19 of the 23 agencies didn't have a documented quality assurance process and 17 lacked uniform methods for identifying cyber workers.

The GAO delivered four recommendations to ONCD, calling on it to work with OMB and agencies on formalizing various data-collection processes and assessing the cost-effectiveness of cyber workforce initiatives. The office did not agree or disagree with the recommendations.

"Until ONCD addresses these factors, it cannot ensure that agencies will have the information needed to support workforce decisions," the GAO concluded. "This is especially important during administration transitions when new leadership needs assurance that the federal government is prepared and cyber-ready.

Note:
Many security controls for Insider Risk Management are the responsibility of the IT Department / Cyber Security Program. If government agencies don't even know what contractors are working for them and what they are doing, how can the agency handle detecting, mitigating and preventing the risks and threats from employees, and threat actors external to the agency? (Source 1) (GAO Report)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

U.S. Navy Admiral Sentenced To Prison For Awarding Contract To Company In Exchange For His Future Employment - September 16, 2025

Admiral Robert P. Burke (USN-Ret.), 62, of Coconut Creek, Florida, was sentenced to prison in connection with accepting future employment at a government vendor in exchange for awarding that company a government contract.

From 2020 to 2022, Burke was a four-star Admiral who oversaw U.S. naval operations in Europe, Russia, and most of Africa, and commanded thousands of civilian and military personnel.

Burke's co-defendants, Yongchul "Charlie" Kim and Meghan Messenger, were the co-CEOs of a company (Company A) and provided a workforce training pilot program to a small component of the Navy from August 2018 through July 2019. The Navy terminated that contract with Company A in late 2019 and directed Company A not to contact Burke directly about contracting actions.

Despite the Navy's instructions, the co-defendants met with Burke in Washington, D.C., in July 2021, to reestablish Company A's business relationship with the Navy.

At the meeting, the co-defendants agreed that Burke would use his position as a Navy Admiral to steer a contract to Company A in exchange for future employment at the company. They further agreed that Burke would later use his official position to influence other Navy officers to award another contract to Company A to train a large portion of the Navy with a value one of the co-defendants allegedly estimated to be in the "triple digit millions."

In December 2021, Burke ordered his staff to award a $355,000 contract to Company A to train personnel under Burke's command in Italy and Spain. Company A performed the training in January 2022.

Thereafter, Burke promoted Company A in a failed effort to convince another senior Navy Admiral to award another contract to Company A. To conceal the scheme, Burke made several false and misleading statements to the Navy, including by falsely implying that Company A's employment discussions with Burke only began months after the contract was awarded and omitting the truth on his required government ethics disclosure forms.

In October 2022, Burke began working at Company A at a yearly starting salary of $500,000 and a grant of 100,000 stock options. (Source)

Employee For Numerous Defense Contractors Sentenced To Prison For Attempted Espionage With Russia - September 15, 2025

John Rowe was employed for nearly 40 years as a test engineer for multiple cleared defense contractors. In connection with his employment, Rowe held various national security clearances from SECRET to TOP SECRET//SCI (Sensitive Compartmented Information) and worked on matters relating to U.S. Air Force electronic warfare technology, among other things. After several security violations and concerning inquiries and statements about Russia and sensitive information, Rowe was identified as a potential insider threat and terminated from employment.

In March 2020, Rowe told an undercover FBI agent, who he believed to be an agent of the Russian government, that he was not loyal to the United States and that he was interested in helping Russia. During this meeting, Rowe disclosed national defense information classified as SECRET that concerned specific operating details of the electronic countermeasure systems used by U.S. military fighter jets, among other things.

Over the course of the next eight months, Rowe exchanged over 300 emails with a person he believed to be a Russian agent, confirming his willingness to work for the Russian government and discussing his knowledge of classified information relating to U.S. national security. In one email, Rowe explained, "If I can't get a job [in the United States] then I'll go work for the other team."

In another email, Rowe disclosed classified national defense information concerning the U.S. Air Force. In September 2020, Rowe had a second in-person meeting with the undercover FBI agent. During this meeting, Rowe again disclosed classified national defense information. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

U.S National Guardsman Is Accused Of 3D-Printing Weapons Parts For Al-Qaeda - September 25, 2025

A 25-year-old former member of the National Guard is accused of attempting to provide 3D-printed weapons to someone he believed was a member of al-Qaeda, according to a criminal complaint.

While serving in the National Guard, Andrew Hastings of Tulsa, Oklahoma, allegedly shipped more than one hundred parts for weapons to an undercover agent with the intent of assisting the radical Islamic terrorist group. He is charged with attempting to provide material support or resources to a designated foreign terrorist organization and illegal possession or transfer of a machine gun.

Hastings first came under FBI scrutiny in June 2024 after he was found to be "discussing committing acts of violence against U.S. civilians in furtherance of global jihad" on a social media app, according to the Justice Department. At the time, he worked as an aircraft powertrain repairer and held a national security clearance.

On social media, Hastings allegedly encouraged others in a group chat discussing acts of terrorism to develop cyberspace skills and start physical training. He allegedly offered to provide Army manuals related to tactics and the manufacture of weapons and expressed interest in creating a nuclear weapon.

Hastings then began conversing with an undercover agent who claimed to have ties to al-Qaeda. Surveillance footage cited in court documents reportedly shows Hastings dropping off boxes at a post office to ship 3D printed machine gun conversion switches, two 3D printed lower receivers for a handgun, a handgun slide, and other handgun parts for "al-Qaida for use in terrorist attacks."

Investigators also stated that he took an overseas trip without reporting it to his superiors as required. Hastings voluntarily left the National Guard on June 6, 2025, as the investigation was ongoing. (Source)

DHS Deportation Officer Sentenced To Prison For Laundering $700,000 In Drug Proceeds - September 16, 2025

Christopher Toral, who is a former DHS Deportation Officer has been sentenced to prison for laundering money while working for the Department of Homeland Security (DHS).

Toral began working with Immigration and Customs Enforcement in 2008 and was assigned to a processing center. Over a two-month period in 2023, he used his position as a federal law enforcement officer to transport $700,000 in drug proceeds under the guise of official duties.

As part of an undercover operation, Toral agreed to transport a black bag containing $200,000 in cash from Dallas to Houston in February 2023, believing the money was from illegal narcotics sales. He made the same trip later that month delivering an additional $200,000.

In March, Toral flew from Newark, New Jersey, to Houston with $300,000 in suspected drug money, bypassing airport security and Transportation Security Administration by exploiting his law enforcement position. Toral did all this in exchange for cash payments. (Source)

2 Police Department Employees (Chief & Captain) Sentenced To Prison For Falsely Claiming $149,000+ Of Overtime Work - September 17, 2025

2 men, the former Chief and Captain of the Bethany Beach Police Department, have been sentenced to terms of imprisonment for theft of federal funds. Michael Redmon, was sentenced to prison, and ordered to pay restitution of $81,890 and a fine of $50,000. Darin Cathell, was sentenced to two months in prison followed by six months of home detention and ordered to pay restitution of $67,790 and a fine of $25,000.

Redmon, the former Chief of the Department, and Cathell, the former Captain of the Department, spent years claiming to work overtime shifts that they did not, in fact, work. Redmon falsely claimed at least 174 overtime shifts, totaling at least 760 hours and at least $81,890. Cathell falsely claimed at least 185 overtime shifts, totaling at least 800 hours and at least $67,970. Some of the funds Redmon and Cathell received were federal grant funds. (Source)

Police Department Employee Accused Of Defrauding Domestic Violence Victims By Taking $6,700 In Bribes - September 3. 2025

A Siler City Police Department employee in North Carolina (NC) is the suspect of a fraud case in which the NC State Bureau of Investigations (SBI) claims she defrauded domestic violence victims she was supposed to be helping.

Gloria Maldonado was the subject of the investigation. The bureau said she is a domestic violence advocate with the police department. The police department said she has been an employee since 2015. The police department was given information regarding Maldonado receiving cash payments for helping people obtain a U-Visa. The department said it recommended the SBI investigate the employee.

U-Visas, according to the U.S. Department of Homeland Security, are visas provided to victims of certain crimes who suffered mental and physical abuse and are assisting or being helpful to law enforcement during the criminal investigation.

Maldonado was charged with taking money in order to assist with U-Visa applications. After receiving the money, however, no assistance was given to the victims, the documents state. In the first charge, Maldonado was said to have taken $1,500 and in the second charge she was said to have taken $5,200.

Other victims have come forward and reported that Maldonado defrauded them as well. Maldonado is currently on non-disciplinary suspension pending the results of the department's internal investigation. (Source)

Police Department Employee Arrested For $6,000 Of Time Card Fraud / Conspired With Supervisor To Falsify Timesheets - September 22, 2025

Eunique Gibbons worked in a civilian role for the Lauderhill Police Department (LPD) in Florida. She turned herself in at the jail to face a felony charge connected with her job.

LPD investigators said Eunique Gibbons, a property and evidence coordinator with the department, conspired with her supervisor (Denesha Moore) to falsify her timesheet. Authorities said she made nearly $6,000 for hours she never worked.

Authorities said evidence showed that Moore clocked Gibbons in 21 times from January to August 2024 in instances where Gibbons didn't show up to work anywhere between one to seven hours later. (Source)

Sheriff's Office Employee Charged For $5,900 Of Bribery Involving $100,000 Of Federal Grant Money - September 3. 2025

Kenneth Lawson worked as Grants Manager in the Orleans Parish Sheriff's Office (OPSO) Grants Department from August 2022 to November 29, 2024. In that role, he could request grant payments and issue checks to subgrantees under OPSO grants.

Lawson met Banks in March 2024, and the two allegedly devised a scheme in which Lawson diverted checks made out to subgrantees into accounts controlled by him or Banks. Banks then allegedly paid bribes to Lawson, including an approximately $5,900 payment on Aug. 12, 2024, stemming from the unauthorized diversion of about $15,000 from OPSO.

The indictment also alleges that on July 30, 2024, Lawson incorporated Williams James Assoc. LLC and opened a business account in its name. He then allegedly directed the U.S. Department of Justice to transfer $100,000 from a $3.9 million DOJ grant to the Williams James account without OPSO approval. To make the transaction appear legitimate, Banks reportedly posed as an OPSO employee when contacting the financial institution. (Source)

Department Of Corrections Officer Sentenced To Prison For Accepting $10,000 Bribe To Smuggle Contraband Into Prison - September 24, 2025

Paul Ketteman was employed as a corrections officer at the Alabama Department of Correction's Limestone Correctional Facility in Harvest, Alabama. Ketteman's job duties included inspecting prison cells for contraband and supervising inmates.

In the Fall of 2022, ADOC's Law Enforcement Services Division began an investigation into contraband being smuggled into the prison facility by a corrections officers. As part of the investigation, Cash App records were obtained for Ketteman's account. These records revealed that in less than three months in 2022, Ketteman was paid more than $10,000 to smuggle contraband into the prison and to act as a lookout. (Source)

Former NYPD Detective Pleads Guilty For Accepting Bribes For Violent Racketeering Conspiracy - September 26, 2025

Saul De La Cruz, is a former NYPD detective.

Saul De La Cruz pleaded guilty to a racketeering conspiracy in connection with his participation in a violent theft crew. De La Cruz, then a member of the NYPD, accepted bribes for providing crew members with confidential police information about potential victims and ongoing investigations. When he learned that the FBI was planning to arrest members of the crew, he tipped them off, allowing them to flee.(Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

Pennsylvania Township Tax Collector Pleads Guilty To Embezzling $400,000+ In Property Taxes - September 23, 2025

From March 2023 to January 2025, John McGinnis was the tax collector for Fairview Township responsible for collecting property taxes from the residents of Fairview Township, including taxes payable to the Township, Luzerne County, and the Crestwood School District.

During that timeframe, McGinnis embezzled more than $400,000 in property taxes and converted them to her own personal use. Both Luzerne County and the Crestwood School District received more than $10,000 from the federal government via grants and other programs during this timeframe. (Source)

Maryland Department Of Labor Contractor Pleads Guilty To Issuing $250,000+ Of Fraudulent Unemployment Insurance Funds To Family Members & Friends In Exchange For Bribes - September 17, 2025

Between June 2020 until about November 2021, Natonia Johnson assisted friends, family members, and strangers with fraudulently filing and obtaining UI benefits they were not eligible to receive in exchange for bribes and kickback payments.

Johnson assisted individuals with uploading fraudulent documents in support of UI claims. She then falsely asserted that these individuals were self-employed. Later, through her employment as a contractor at Company #1, Johnson staffed MD-DOL's UI call center and gained access to MD-DOL's internal UI database. Then Johnson used this access to remove flags and holds on various co-conspirators' UI accounts that established these individuals were ineligible to receive UI benefits. Additionally, Johnson backdated claims, removed fraud holds, and caused MD-DOL to issue additional UI benefits that these co-conspirators were ineligible to receive. In exchange, Johnson received between $200 and $500 from each co-conspirator whose claims she assisted with. Through the scheme, Johnson defrauded the MD-DOL of more than $250,000 in UI claims. (Source)

County Director Of Finance Sentenced To Prison For Stealing $125,000+ In Public Funds / Useds Funds To Live Lavish Lifestyle - September 2, 2025

Regene Newman exploited positions of public trust over a period of more than seven years, stealing over $125,000 intended for community programs and nonprofit organizations. She used the funds to support a lavish lifestyle, making large purchases at retailers including Sephora, Ulta Beauty, Bath & Body Works, Bra Goddess, Hobby Lobby, Target, and Macy's.

From 2015 to June 2021, Newman served as Director of Finance for the Vanderburgh County Prosecutor's Office in Indiana, where she had authorized access to both an office credit card and a debit card for My Goals, a nonprofit operating under the Prosecutor's Office to assist at-risk youth.

Between March 2016 and March 2021, Newman made approximately $60,028.66 in unauthorized purchases with the My Goals debit card. To conceal the theft, she arranged for the Prosecutor's Office to make sham "donations" to the nonprofit by submitting false Accounts Payable Vouchers. These fake donations created the appearance that the funds would be used to support My Goals' mission of helping the community. During that time, Newman also made $26,381.04 in unauthorized purchases using the Prosecutor's Office credit card.

In June 2021, Newman left the Prosecutor's Office and became Business Director for Vanderburgh County Community Corrections. There, she gained access to a separate county credit card and later requested responsibility for managing the checking account of a local nonprofit that supports individuals battling addiction. Once granted access, she made an additional $10,725 in unauthorized credit card purchases and $23,929.46 in unauthorized debit card purchases. (Source)

Florida State Housing Authority Employee Pleads Guilty To $155,000+ Theft Of Federal Funds / Used For Personal Benefit - September 19, 2025

Thomas Hoffman was an employee of the Palatka Housing Authority (PHA), which received federal funds from the United States Department of Housing and Urban Development (HUD) to administer public housing programs in Palatka and neighboring municipalities. Hoffman was responsible for information technology and accounts payable.

During an audit of vendors in 2025, PHA identified an unapproved company called "Data Max," which had received approximately 48 fraudulently issued payments from PHA's general account between July 2023 and

February 2025, totaling $155,706. A federal investigation determined that Hoffman owned and controlled Data Max and its corporate bank account, and that Hoffman had caused the fraudulent payments to be issued. The investigation showed that Hoffman used the funds for his personal benefit. Bank surveillance footage obtained by investigators showed Hoffman cashing PHA checks issued to Data Max on numerous occasions.
(Source)

Louisiana Department Of Education Employee Pleads Guilty To Stealing $74,000+ Of Grant Money - September 12, 2025

From April 2020 and continuing to at least March 29, 2021, Romney Manuel conspired with another to devise a scheme to obtain federal funds in the form of LaCAP grant money from the Louisiana Department of Education. During the course of said conspiracy, Manuel and his co-conspirator made a non-existent childcare provider appear operational and manipulated spreadsheets and data systems utilized by the Louisiana Department of Education in order to steal $74,250 in federal funds. (Source)

Executive Director Of State Liquor Control Commission Charged For Providing Illegal Assistance To Adult Night Club Owners And Extorting Business Owner For $65,000 - September 25, 2025
Hobert Rupe is the former Executive Director of the Nebraska Liquor Control Commission.

Rupe is alleged to have violated his oath of office as the Executive Director of the Nebraska Liquor Control Commission when he allegedly conspired with adult establishments' owners to include Brent Zywiec to receive a stream of significant personal and financial benefits in exchange for illegal assistance he provided the owners of the establishments. The alleged stream of benefits included commercial sex acts, cash, and free benefits at the clubs that others pay to receive such as VIP dances, alcoholic drinks, and cover charges. In exchange for these benefits, Rupe would fail to report or investigate numerous liquor license violations that occurred at each establishment and would separately abuse law enforcement resources in an attempt to harm Zywiec's competitors in Omaha.

Finally, there is a count of the Indictment that alleges Rupe extorted a business owner in the community for $65,000 with the understanding that Rupe would provide assistance with helping that business owner retain a liquor license that the business owner would not otherwise qualify for under state rules and regulations. (Source)

New York City Board Of Elections Employee Sentenced To Prison For $40,000+ Extortion And Fraud Scheme - September 2, 2025
Nicole Torres is a former elected district leader in the Bronx and employee of the New York City Board of Elections (NYC-BOE).

She was sentenced to two years in prison for participating in conspiracies to commit extortion and mail fraud for illegally demanding payments from Bronx residents in exchange for selecting those individuals as poll workers and for agreeing with others to falsify documents to make it appear that certain individuals had worked as poll workers when they had not. Based on her participation in the various schemes Torres personally earned at least approximately $40,970. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

School Employee Sentenced To Prison For Embezzling $30,000+ From School District / Used Funds For Personal Benefit - September 16, 2025
Jonnie Eagle, while working for the Heart Butte School District, Montana, embezzled funds by using school credit cards and purchase orders, presenting such orders to local grocery stores, and obtaining and using gift cards for her own personal benefit, none of which was authorized. While doing so, Eagle forged the name of school employees to cover up the fraudulent transactions. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

Bank Chairman Of The Board Pleads Guilty To $13 Million+ Wire Fraud Conspiracy That Led To Bank's Collapse - September 24, 2025

The chairman of the board of Nodus International Bank (Nodus), a Puerto Rican international banking entity, pleaded guilty for his role in leading a scheme to fraudulently obtain more than $13.6 million from Nodus, which ultimately led to the bank's failure in 2023.

Juan Ramirez conspired with others to siphon money from Nodus. Ramirez and a co-conspirator concealed from other Nodus board members and executives, and the bank's regulator that certain investments or loans were for the benefit of Ramirez and a co-conspirator, in violation of Puerto Rican law and Nodus policy regarding insider transactions. (Source)

Bank Executive Sentenced To Prison For Stealing $2.4 Million / Used Funds For Personal Expenses - September 18, 2025

Andrew Blassie served as the Executive Vice President for the Bank of O'Fallon in Illinois. He defrauded the bank out of $1,972,887.67 in a check kite scheme from September 2023 through September 2024 during his employment.

Blassie admitted to falsely inflating the balance of his personal checking account at the Bank of O'Fallon by depositing checks he knew to be backed by non-sufficient funds. He deposited checks with non-sufficient funds from four personal accounts at three other banks and one credit union into the Bank of O'Fallon account.

Blassie paid nearly $2.7 million for personal expenses from the falsely inflated account thus using funds belonging to the Bank of O'Fallon. As the former Executive Vice President, Blassie used his position to conceal his fraud from the Bank of O'Fallon by scrubbing his name and account number from suspected kiting reports.

Blassie was ordered to pay $2,461,887.67 in restitution. (Source)

Bank Employee Sentenced To Prison For Stealing $158,000+ From Customer Accounts / Used Funds For High Priced Technology Items & Gambling - September 16, 2025

Between January 2023 and March 2024, Dekoda Clark was employed as a Relationship Banker at a bank branch in Evansville, Indiana. During this time, Clark exploited his position to steal approximately $158,208.53 from customer accounts by making unauthorized cash withdrawals and issuing fraudulent debit cards.

Leveraging his access, Clark created debit cards linked to the checking accounts of five individuals and two businesses without their knowledge or consent. He then used these cards to make 17 purchases at various retailers, including Dicks Sporting Goods, Guitar Center, and Best Buy. Several of the purchases were for high-value technology items, including three Apple iPads, a MacBook Pro, an Apple Watch Ultra, two large televisions, a Lenovo gaming laptop, memory cards, a DJI Mini Drone, and an Xbox game drive. One of the transactions was for a $2,000 deposit into Clark's account with Draft Kings, an online sports betting platform. These fraudulent purchases totaled $15,708.53.

Clark also withdrew a total of $142,500 as cash from the checking accounts of three individuals without their knowledge or consent. (Source)

Coinbase Data Breach Costs $400 Million / Caused By Coinbase Contractor That Used Cell Phone To Take Pictures And Sell Data To Hackers - September 17, 2025

A newly unsealed court filing has revealed the most detailed account yet of the massive data breach that struck Coinbase earlier this year, exposing more than 69,000 users and causing damages estimated at $400 million.

The documents allege a coordinated scheme led by an employee of TaskUs, the customer service outsourcing firm hired by Coinbase, and accuse the TaskUs of concealing the extent of the incident. According to the court filing, Ashita Mishra, an employee at TaskUs's Indore office in India, began stealing sensitive customer data in September 2024.

Using her phone, Mishra allegedly photographed up to 200 customer records per day, including names, emails, addresses, bank account details, balances, and even Social Security numbers. The stolen information was sold to hackers for $200 per image, who then used it to impersonate employees at the leading American crypto exchange and defraud users

By the time Mishra was arrested in January 2025, her personal device reportedly contained data from more than 10,000 customers. Investigators allege Mishra recruited supervisors and team leaders, turning the theft into a hub-and-spoke conspiracy within the TaskUs workforce.

The complaint expands the case beyond insider misconduct, accusing TaskUs of negligence, fraud, and a deliberate effort to suppress the breach.

TaskUs fired 226 employees and later dismantled its human resources investigation team in an attempt to silence those with knowledge of the breach. (Source)

Bank Employee Accessed Data For 689,000 Customers For 1 Year After Leaving Bank - September 17, 2025

FinWise Bank, a Utah-based community bank, recently suffered an insider data breach when a former employee accessed sensitive customer data after their employment had ended.

In a new report filed with the Office of the Maine Attorney General, FinWise said that the breach happened on May 31, 2024, but was discovered more than a year later, on June 18, 2025. In total, sensitive data on 689,000 people was compromised. (Source)

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

Medical Center Board Of Trustees Member And Employee Arrested For Submitting $1.2 Million Of Fraudulent Invoices To Hospital - September 22, 2025

A former North Sunflower Medical Center (NSMC) Board of Trustees member (Chris Waldrup) and his employee (Phil McNeer) were arrested for submitting fraudulent invoices, according to the State Auditor's Office.

State Auditor Shad White said McNeer, the former board member, and Waldrup concealed the true identity of McNeer's business through the submission of fraudulent invoices to the NSMC under Waldrup's name.

McNeer and Waldrup are accused of submitting 216 fraudulent invoices between March 2015 and March 2025, causing the hospital to make payments to, and for the benefit of, businesses owned by McNeer.

As a NSMC board member, White said McNeer was prohibited by law from using his position to benefit himself or any business he is associated with. The State Auditor's Office issued a $1.2 million demand to McNeer and Waldrup. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Biotech Company Arcturus Therapeutics Is Suing AbbVie For Hiring Former Employees Who Stole Trade Secrets - September 23, 2025

Arcturus alleged in the lawsuit, that AbbVie subsidiary Capstan Therapeutics hired away an Arcturus employee and a consultant who took company secrets concerning lipid nanoparticle (LNP) technology and shared them with their new employer.

The lawsuit said that Capstan hired away former Arcturus employee Priya Karmali and consultant Steven Tanis in 2022. Arcturus' alleges that Karmali and Tanis took trade secrets to Capstan related to the use of LNPs to transport RNA into the human body. Arcturus said Capstan applied for an LNP-related patent shortly after hiring Karmali and Tanis that listed them as its inventors and included Arcturus' trade secrets. (Source)

Elon Musk's Artificial Intelligence Startup xAI Wins Court Order Blocking A Former Employee From Collaborating With Rival Compitor OpenAI - September 4, 2025

In a lawsuit filed in California last month, xAI accused one of its founding team of engineers who worked on Grok of "willful and malicious misappropriation of xAI's confidential information and trade secrets."

The lawsuit states that Xuechen Li copied trade secrets from his company laptop to personal storage systems, in violation of the terms of his employment. These allegedly included "cutting-edge AI technologies with features superior to those offered by ChatGPT and other competing products."

According to xAI, Xuechen Li copied trade secrets the same day he received millions of dollars in company stock. Three days later, he "suddenly resigned," the suit states. (Source)

Elon Musk's Artificial Intelligence Startup Is Suing xAI For Hiring Former Employees Who Stole Trade Secrets - September 25, 2025

Elon Musk's artificial intelligence startup xAI has sued rival OpenAI in California federal court for allegedly stealing its trade secrets to gain an unfair advantage in the race to develop AI technology.

The lawsuit opens new tab said that OpenAI was engaged in a "deeply troubling pattern" of hiring away former xAI employees to gain access to trade secrets related to its AI chatbot Grok. According to the complaint, OpenAI hired away former company engineer Jimmy Fraiture and an unnamed senior finance executive in addition to Li in order to obtain xAI trade secrets.

xAI said it discovered the alleged campaign to undermine the company after bringing allegations of trade secret theft against former engineer Xuechen Li, who it has accused of taking confidential information to the ChatGPT maker in a separate lawsuit. (Source)

Scale AI Files Lawsuit Against Former Employee Who Stole 100+ Confidential Documents / Trade Secrets - September 3, 202

Scale AI, which helps tech companies prepare data to train their AI models, filed a lawsuit against one of its former sales employees and its rival Mercor on Wednesday. The suit claims the employee, who was hired by Mercor, "stole more than 100 confidential documents concerning Scale's customer strategies and other proprietary information.

Scale is suing Mercor for misappropriation of trade secrets and is suing the former employee, Eugene Ling, for breach of contract. The suit also claims the employee was trying to pitch Mercor to one of Scale's largest customers before he officially left his former job.

Mercor co-founder Surya Midha denies that his company used any data from Scale, although he admits that Ling may have been in possession of some.

Ling stated on X, "Just heard I'm getting sued by Scale. Last month, I left Scale to work at Mercor. I know this was frustrating for my old team, and I feel bad about that."

"When Scale reached out about some files I had in my personal drive, I asked if I could just delete them. But Scale asked that I not do anything with them, so I'm still waiting for guidance on how to resolve this. I've never used any of them in this role. It sounds like Scale wants to sue me and that's up to them.

But I just wanted to say that there truly was no nefarious intent here. I'm really sorry to my new team at Mercor for having to deal with this." (Source)

NOTE:

Employee Seperation From Company - A Chance To Surrender Company Information

This was great advice from an Insider Threat Program Manager that spoke at the 2019 Insider Threat Symposium & Expo.

Consider Including This Key Verbiage In Employee Off Boarding Briefings (Separations, Terminations, Workforce Reductions)

Example: "We know that many employees store work related and personal information on company issued computer systems / electronic devices, to include personal electronic devices.

Our experience has shown that during the off boarding process, employees often inadvertently mix sensitive company data in with personal data when downloading in preparation for departure. If you have downloaded any company information to your personal electronic devices, sent it via personal e-mail, or stored it in your personal cloud storage, please allow us to examine that information to ensure no company owned data was inadvertently included. This will avoid delays or complications in the off boarding process based upon our data security review".

Note:

Often people will self-surrender storage devices based on this verbiage. It is most effective if it is read aloud to them. Also have them sign and agree to the above statement. If employees are surrendering removable media and thanking your team for keeping them out of trouble, you are making headway in your Insider Threat mitigation efforts.

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

CEO Of Internet Service Provider Sentenced To Prison For Stealing $600,000+ - September 19, 2025

From January 2017 through January 2023, Anthony Lang devised and executed a scheme to defraud his employer, a telecommunication and internet service provider.

At the time of the scheme, Lang was the CEO of the company and had access to their books and accounts. Over a six-year time period, Lang stole over $600,000 from the company. (Source)

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

Bookkeeper For Company Sentenced To Prison For Embezzling $9.8 Million / Used Funds For Gambling - September 18, 2025

Hava Austin owned and operated Accounting Solutions Today, P.A., a bookkeeping and tax services business in Broward County, Florida. Austin was also the long-time bookkeeper for the victim company, where she had signature authority over its bank accounts.

From 2018 through April 2024, Austin embezzled approximately $9.8 million. Austin executed unauthorized wire transfers from the victim company's accounts to her own business and used much of the stolen money to gamble at local casinos and through online gaming platforms.

To conceal her theft, Austin falsified accounting entries in the victim company's ledgers, often creating fraudulent entries under fake but similar-sounding vendor names. (Source)

Law Firm Employee Sentenced To Prison For Embezzling $2.7 Million+ / Used Funds For Gambling - September 17, 2025

Destiny Combs was the Accounting Manager for a surrogacy agency and affiliated law firm.

Between February 2019 and June 2023, Combs embezzled approximately $2.72 million from the businesses. Combs's scheme was simple: she used personal credit cards to fund her gambling habit, then used company funds to pay her credit card bills. Combs stole the money to fuel her online gambling addiction. She made fraudulent entries in the companies' books to disguise her credit card payments as business expenses, and exploited the trust and autonomy her company gave her to go undetected. Over 52 months, Combs made approximately 292 payments from the company accounts to her personal American Express credit card, totaling $2,723,025. Combs gambled away most of the $2.7 million she stole. (Source)

Employee For Non-Profit Organization Sentened To Prison For Embezzling $2.3 Million+ / Used funds For Remodeling Home, Mortgage, Credit Card & Car Payments - September 11, 2025

Marcia Joseph was a former senior fiscal officer for a non-profit organization. Joseph admitted stealing $2,339,700 from the Non-Profit and funneled the funds to a sham company she had set up.

The invoices described services purportedly provided in connection with a New York City Department of Education educational program focusing on students in shelters and, later, job training for adults in shelters. Over the course of nearly 17 years, Joseph generated and submitted more than 500 fictitious invoices and manipulated the Non-Profit's accounting systems to avoid detection.

She used the stolen funds to pay for numerous personal expenses, including approximately $235,000 in mortgage payments, $207,000 in credit card payments, $98,000 in car payments, $45,000 in Amazon expenses, and various other personal items, such as home remodeling, spa treatment, landscaping expenses, and luxury goods. (Source)

Company Manager Pleads Guilty To Stealing $1.6 Million From Customer Credit Accounts / Used Funds His Wedding, Vacation, Etc. - September 25, 2025

Tony Ream pleaded guilty to wire fraud committed in connection with his employment as a credit supervisor for a Long Island Company.

Over the course of four years, Ream sent wire transfers totaling approximately $1.6 million from the Company's bank account to a bank account that he controlled, and used those funds for his own personal gain. Ream spent the stolen funds on his wedding, luxury international vacations, and a failed restaurant venture in South Carolina. (Source)

General Manager Admits Embezzling $878,000 From Her Employer / Used Funds To Pay Credit Card Bills - September 2, 2025

Kristina Higgins is the former general manager of a Missouri company.

Higgins admitted issuing company checks to pay a total of $878,711 in personal credit card bills and using a stamp to add the company owner's signature on the checks. In December of 2022, she falsified information to ensure that the checks would be honored when the company enrolled in the bank's positive pay system. (Source)

Company Bookkeeper Pleads Guilty To Embezzling $860,000+ From 2 Different Employers / Used Funds For Personal Expenses - September 9, 2025

Fom mid-2018 to April 2022, Marie Higgins was employed as a bookkeeper for New England Kitchen & Bath LLC in Glastonbury.

Higgins stole from the business by issuing company checks payable to herself, often including the words "commission" or "bonus" in the memo line of the check, and used a signature handstamp of the company's owner to issue the checks; initiating wire transfers to bank accounts in her name; creating a fictitious supplier and billing the company for fictious expenses; using company debit cards to pay for personal expenses; and

overseeing a construction proposal for a legitimate client project, expensing incurred costs of the project through the company, and having the client pay her directly. Higgins stole $504,807 through this scheme.

From February 2023 to April 2024, Higgins was employed as an accounting manager for PVC Solutions, Inc., in Danbury, a company that produces and distributes PVC products.

Higgins stole from the company by issuing company checks payable to herself; creating duplicate vendor payment templates to initiate wire transfers to her personal bank account; creating fictitious suppliers to bill the company on her behalf; and paying personal expenses through the company's bank account. Higgins manipulated the company's accounting records to conceal her criminal activity. Higgins stole $356,181 through this scheme. (Source)

Insurance Company Claims Adjuster Found Guilty Of Stealing $580,000+ / Used Funds For Designer Clothing, Jewelry, Etc. - September 19, 2025

Between March 2021 and February 2022, Octavias Owens defrauded his employer, a regional insurance company, out of more than $580,000.

Owens, who worked as a claims adjuster at the company, would reopen claims files that had already been settled and paid out. He would upload "comparative estimates" that he created to the claim files to make it look like additional work had been done. Owens would then cause checks to be issued on the claims to a shell company that he controlled that was disguised as a construction and roofing company. After the checks were issued, Owens would cash the checks at Orlando-area ATMs. He then used the proceeds for his own personal benefit, including to purchase designer clothing, jewelry, hotel rooms, vehicle accessories, and other luxury items. (Source)

Director Of Finance & Human Resources Sentenced To Prison For Stealing Nearly $540,000+ / Used Funds For Travel, Clothing, Rent Payments, Etc. - September 18, 2025

Joelle Fouse was the manager / director of finance and human resources for Promise Community Homes, formerly known as Rainbow Village(RV) in Missouri from 2012 to 2023. RV is a charity that provides housing and resources for adults with intellectual and developmental disabilities. She was responsible for payroll, expense reimbursement and maintaining the charity's books and records.

Fouse caused 71 unauthorized payroll deposits totaling $139,810 and 181 unauthorized expense reimbursement payments totaling $407,186 to be made to her personal bank accounts. She also used the charity's credit card to make 184 unauthorized personal purchases totaling $133,210. Her theft, and the unauthorized payments, caused the charity to overpay payroll taxes by approximately $10,694. She pleaded guilty in April of 2025 to three felony counts of wire fraud.

Fouse used the money to pay for personal expenses for herself and relatives including travel, clothing, entertainment, restaurants and rent payments. To cover up her crimes, she created false financial reports, doctored receipts, made false entries in the charity's financial records and prevented the charity's officials from accessing records which would have disclosed her scheme. (Source)

Business Manager For Private School Pleads Guilty To Embezzling $239,000+ / Used Funds For Travel, Concerts, Rent, Etc. - September 4, 2025

From May 2021 through June 2024, Shannel Hilliard, 46, was the business manager for a private school in Richmond, Virginia. As business manager, Hilliard's responsibilities included management and maintenance of the school's books and records, performance of periodic bank reconciliation reports, and making purchases and payments on behalf of the school. As part of those responsibilities, Hilliard had control of a credit card in the school's name for official school business only.

From November 2021 through July 2024, Hilliard used the school's credit card to pay for personal expenses, including trips to Orlando, Las Vegas, Myrtle Beach, and Miami; performances such as Hamilton and concerts such as Usher, LL Cool J, and Capitol Jazz; luxury goods such as purses and jewelry; and rent for Hilliard's personal residence. On May 24, 2024, Hilliard used the credit card for a $1,591.77 payment to the Boathouse at Rocketts Landing for a personal graduation party.

Hilliard attempted to conceal her embezzlement by falsifying the school's bank reconciliation reports, including misrepresentations that certain expenses fell under categories of approved spending.

For example, Hilliard attributed personal expenses such as a cruise on Royal Caribbean, a hotel stay in Winston-Salem, North Carolina, and a deposit to the Boathouse at Rocketts Landing to category for ongoing construction at the school. (Source)

Former Ronald McDonald House Director Accused Of Stealing $120,000+ From Charity / Deposited Funds Into Her PayPal Accounts - September 25, 2025

The former executive director of Ronald McDonald House Charities of Marshfield, Wisconsin, is facing felony charges for stealing more than $100,000 from the organization.

Iilee Pederson, who resigned her position on June 26, 2024, is charged with money laundering, five counts of making fraudulent writings, three counts of theft in a business setting and two counts of misdemeanor theft.

Pederson had been withdrawing money from the Ronald McDonald House checking account and depositing it into her personal PayPal account, according to the criminal complaint. An accounting firm had found discrepancies between the charity's Associated Bank checking account and statements provided by Pederson while she was executive director.

Pederson was the only one reviewing and approving statements and the reports were saved to a PDF and then recycled, leaving no paper trail, according to the complaint. The Ronald McDonald House Board did not give anyone permission to withdraw money from the account and deposit it into a PayPal account. (Source)

Head Of Equity Trading For Investment Company Sentenced To Prison For Insider Trading / Made Profit Of $220,000+ - September 23, 2025

Working from his home, Ryan Squillante was employed as the Head of Equity Trading at an investment company headquartered in Denver, Colorado. In his position, Squillante received material non-public information (MNPI) about various publicly traded companies.

On 15 different occasions between August 2022 and May 2023, Squillante used MNPI for his own benefit by executing transactions in securities of these companies, making a total profit of $220,912. (Source)

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

Financial Director For Company Charged For Misappropriating $8.2 Million Over 10 Years To Fund His Personal Business - September 23, 2025

Jordan Khammar is charged with wire fraud and money laundering for his role in a decade-long scheme to defraud a multinational media, brand management, and consulting company and stealing over $8.2 million.

Khammar was hired as a financial consultant in 2006 by a multinational media, brand management, and consulting company (Company-1).

He eventually became the company's Financial Director with access to and control over a wide range of its financial accounts and systems including those tied to banking, accounting, bookkeeping and payroll functions. Between January 2015 and May 2025, Khammar abused that access and control to engage in a scheme to defraud Company-1 out of millions of dollars.

During the 10-year period, Khammar initiated over 300 fraudulent wire transactions, sending himself more than $8.2 million dollars from Company-1's bank account.

Khammar wired most of the stolen money to an account held in the name of Olive Tree Ventures, Inc. (Olive Tree), a company that he founded, owned, and controlled. From the Olive Tree account, Khammar dispersed a large portion of the funds to finance his independent business ventures including his media production company, Sideswipe Media, Inc. (Source)

SHELL COMPANIES / FRAUDULENT INVOICE BILLING SCHEMES

2 Executives Sentenced To Prison For $1.9 Million Fraudulent Invoicing & Shell Company Scheme / Used Funds For Luxury Vehicles, Credit Card Payments, Etc. - September 8, 2025

From 2013 to 2020, Michael Vergato served as a vice president at Arrow Electronics, where he oversaw performance tuning of the company's Oracle EBS databases, including work performed by Mark Perlstein's company.

Vergato and Perlstein devised a scheme to bill the data management company for performance tuning services purportedly to be completed by a shell company created by Vergato, Oracle Performance Tuning and Optimization, LLC (OPTO). Posing as a legitimate contractor, OPTO submitted 21 fraudulent contracts and invoices to the data management company for database performance tuning services that were never performed. Perlstein, in his position as CEO, approved the invoices and wired payments to OPTO.

The scheme funneled nearly $2 million in company funds into OPTO. Perlstein and Vergato divided the proceeds, concealing their involvement by using personal email accounts, other corporate entities, and fake identities.

To conceal his role, Vergato used his stepdaughter's identity to conduct business on behalf of OPTO. At trial, the data management company's current CEO testified that the company could not substantiate any work performed by OPTO or identify any actual employees or contractors related to that entity. Tax records confirmed OPTO paid no salaries and issued no contractor forms.

In total, the data management company paid OPTO $1,949,023. Of that amount, Vergato retained approximately $874,000, using the funds for luxury vehicles, credit card payments, retirement accounts, and rent. Perlstein personally received more than $1 million through the scheme. (Source)

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

Investment Firm Employee Charged With Securities And Wire Fraud For Manipulating Computer Based Algorithmic Investment Models - September 11, 2025

Jian Wu is charged with engaging in a scheme to defraud his employer, a New York-based investment management firm (Firm), by secretly manipulating computer-based algorithmic investment models that were used to execute securities trading strategies at the Firm.

Between 2021 and 2023, Wu deceived the Firm by manipulating trading models he created in order to increase his own compensation.

Specifically, Wu designed models, which were approved and released for use, and then covertly made post-release changes to the models' parameters, which significantly altered the models' behavior.

Wu also secretly tested his models on data sets that misrepresented how the models would perform once approved and released. As a result of these changes and misrepresentations, the Firm rewarded Wu with an inflated year-end compensation of approximately $23 million. Wu then used a portion of his compensation to purchase a multimillion-dollar apartment in Manhattan.

When the Firm uncovered Wu's scheme, Wu made additional unauthorized changes to the models' parameters in an attempt to conceal his prior tampering. The Firm fired WU in 2024. (Source)

THEFT OF ORGANIZATIONS ASSESTS

Employee Working For Multinational DVD Company Sentened To Prison For Stealing, Selling Pre-Release Commercial DVDs For Blockbuster Films - September 11, 2025

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

From approximately February 2021 to March 2022, Hale allegedly stole numerous "pre-release" DVDs and Blu-rays, that is, discs being prepared for commercial distribution in the United States and not available for sale to the public. These included DVDs and Blu-rays for such popular films as "F9: The Fast Saga," "Venom: Let There Be Carnage," "Godzilla v. Kong," "Shang-Chi and the Legend of the Ten Rings," "Dune," and "Black Widow."

Hale allegedly sold the DVDs and Blu-rays through e-commerce sites. At least one pre-release Blu-ray that Hale allegedly stole and sold, "Spider-Man: No Way Home," was "ripped" — that is, extracted from the Blu-ray by bypassing the encryption that prevents unauthorized copying — and copied.

That digital copy was then illegally made available over the internet more than a month before the Blu-ray's official scheduled release date. Copies of "Spider-Man: No Way Home" were downloaded tens of millions of times, with an estimated loss to the copyright owner of tens of millions of dollars. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG & ALCOHOL RELATED INCIDENTS

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

Employee Must Pay For $300,000 In Damages He Caused To Winery By Draining Thousands Of Gallons Of Wine / Angry Because Of How Much He Was Paid - September 3, 2025

A former Sparkman Cellars employee who caused $300,000 in damage by draining thousands of gallons of wine at the Woodinville winery has pleaded guilty to restitution but no jail time.

Mark Griswold admitted to criminal trespass in the first degree and malicious mischief in the third degree. A judge ordered him to pay nearly $50,000 in restitution, undergo a mental health evaluation within 30 days, and stay away from the winery's owners and staff.

Prosecutors said Griswold committed the act of vandalism just before Thanksgiving 2023, about 14 months after leaving his job at the family-owned winery. Surveillance footage showed him wearing a mask and using an employee access code to enter the barrel room. In six minutes, he opened valves on two tanks, releasing roughly 2,300 gallons of wine before slipping out the back door.

Griswold had worked at Sparkman Cellars for about a year before leaving in September 2022. According to investigators, he "felt angry about how much he was being paid and harbored resentment and anger toward the winery owner."

"According to the Sparkmans' victim impact statement, he had asked for a 25% raise, and they were not financially able to do that, but they said they met him halfway and did give him a raise, and they could have another conversation later that year," said Senior Deputy Prosecuting Attorney Stephanie Sato. "And then he quit two weeks after that, in the middle of harvest, which is a very crucial time." The destruction left a deep mark on the winery, Sato added. (Source)

EMPLOYEES INVOLVED IN ROBBING EMPLOYER

No Incidents To Report

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'

Store Owner And Employee Arrested For Racially Motivated Attack Against Another Employee - September 3, 2025

A store owner in Greece and one of his employees have been arrested on suspicion of carrying out a racially motivated attack against a coworker.

The incident occurred on the night of September 16–17. The 58-year-old store owner allegedly grabbed a 26-year-old employee, who is a foreign national, by the neck and punched him during a dispute over his employment status. He is also accused of making derogatory remarks about the worker's ethnicity.

At the owner's request, a 23-year-old employee allegedly locked the store to prevent the assault from being noticed and temporarily confiscated the victim's phone.

Both suspects were brought before a prosecutor and face charges of racially motivated dangerous bodily harm, insults, threats, unlawful detention and assault. (Source)

EMPLOYEES' INVOLVED IN TERRORISM

No Incidents To Report

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

INSIDER THREATS DEFINITION / TYPES

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

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

WHO CAN BE AN INSIDER THREAT?

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

INSIDER THREAT DAMAGING ACTIONS CONCERNING BEHAVIORS

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

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

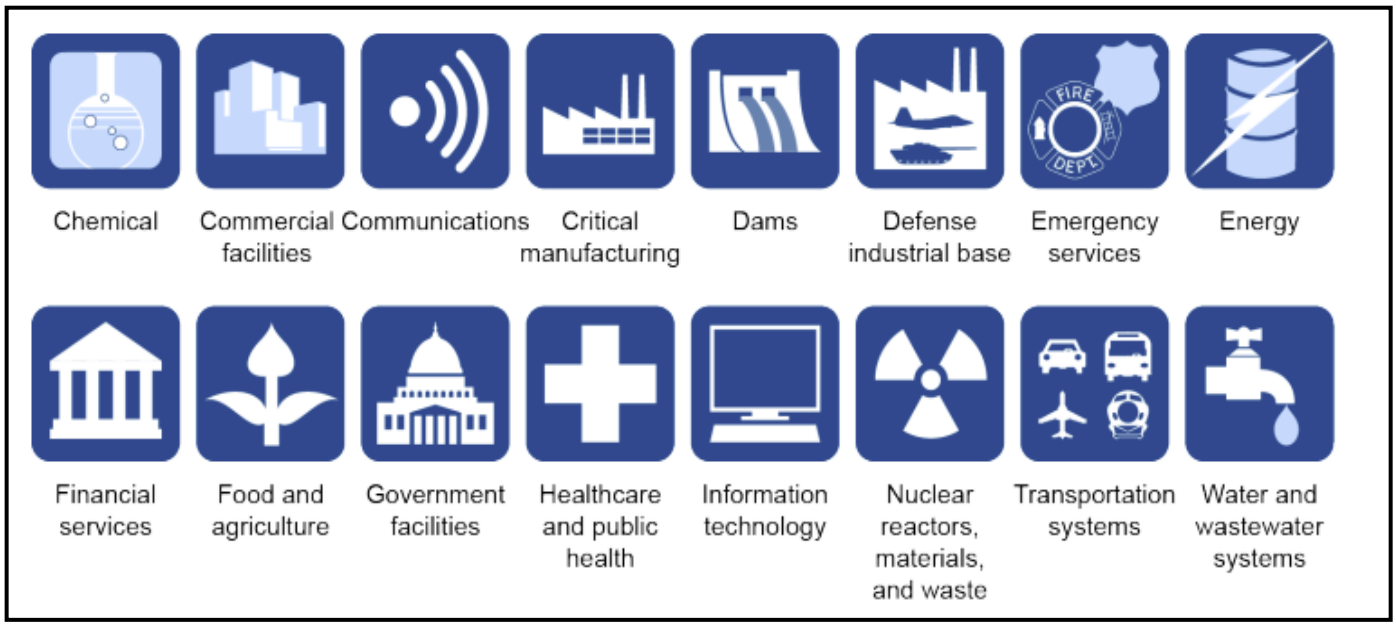
Other Damaging Impacts To An Employer From An Insider Threat Incident

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

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

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

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



WHAT CAN MOTIVATE EMPLOYEES TO BECOME INSIDER THREATS?

EMPLOYER – EMPLOYEE TRUST RELATIONSHIP BREAKDOWN

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

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

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

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

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

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

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

DISSATISFACTION, REVENGE, ANGER, GRIEVANCES (EMOTION BASED)

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

MONEY / GREED / FINANCIAL HARDSHIPS / STRESS / OPPORTUNIST

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

IDEOLOGY

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

COERCION / MANIPULATION BY OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

- ☐ Bribery, Extortion, Blackmail

COLLUSION WITH OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

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

OTHER

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

NITSIG research indicates many employees may not be disgruntled, but have other motives such as financial gain to live a better lifestyle, etc.

You might be shocked as to what employees do with the money they steal or embezzle from organizations and businesses, and how many years they got away with it, until they were caught. (1 To 20 Years)

What Do Employees' Do With The Money They Embezzle / Steal From Federal / State Government Agencies & Businesses Or With The Money They Receive From Bribes / Kickbacks?

They Have Purchased:
Vehicles, Collectible Cars, Motorcycles, Jets, Boats, Yachts, Jewelry, Properties & Businesses

They Have Used Company Funds / Credit Cards To Pay For:
Rent / Leasing Apartments, Furniture, Monthly Vehicle Payments, Credit Card Bills / Lines Of Credit, Child Support, Student Loans, Fine Dining, Wedding, Anniversary Parties, Cosmetic Surgery, Designer Clothing, Tuition, Travel, Renovate Homes, Auto Repairs, Fund Shopping / Gambling Addictions, Fund Their Side Business / Family Business, Grow Marijuana, Buying Stocks, Firearms, Ammunition & Camping Equipment, Pet Grooming, And More.....

They Have Issued Company Checks To:
Themselves, Family Members, Friends, Boyfriends / Girlfriends

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS 2024 REPORT ON FRAUD

If you are an Insider Risk Program Manager, or support the program, you should read this report. Insider Risk Program Managers should print the infographics on the links below, and discuss them with the CEO and other key stakeholders that support the Insider Risk Management Program. If there is someone else within the organization who is responsible for fraud, the Insider Risk Program Manager should be collaborating with this person very closely.

The traditional norm or mindset that malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. There continues to be a drastic increase in financial fraud and embezzlement committed by employees'.

Could your organization rebound / recover from the severe impacts that an Insider Threat incident can cause?

Has the Insider Risk Program Manager conducted a gap analysis, to analyze the capabilities of your organizations existing Network Security / Insider Threat Detection Tools to detect fraud?

Can your organizations Insider Threat Detection Tools detect an employee creating a shell company, and then billing the organization with an invoice for services that are never performed?

This report states that more than half of frauds occurred due to lack of internal controls or an override of existing internal controls.

This report is based on **1,921** real cases of occupational fraud, includes data from **138** countries and territories, covers **22** major industries and explores the costs, schemes, victims and perpetrators of fraud. These fraud cases caused losses of more than **$3.1 BILLION**. (Download Report)

Key Findings From Report / Infographic
Fraud Scheme Types, How Fraud Is Detected, Types Of Victim Organizations, Actions Organizations Took Against Employees, Etc. (Source)

Behavioral Red Flags / Infographic
Fraudsters commonly display distinct behaviors that can serve as warning signs of their misdeeds. Organizations can improve their anti-fraud programs by taking these behavioral red flags into consideration when designing and implementing fraud prevention and detection measures. (Source)

Profile Of Fraudsters / Infographic
Most fraudsters were employees or managers, but **FRAUDS PERPETRATED BY OWNERS AND EXECUTIVES WERE THE COSTLIEST**. (Source)

Fraud In Government Organization's / Infographic

How Are Organization Responding To Employee Fraud / Infographic
Outcomes in fraud cases can vary based on the role of the perpetrator, the type of scheme, the losses incurred, and how the victim organization chooses to pursue the matter. Whether they handle the fraud internally or through external legal actions, organizations must decide on the best course of action. (Source)

Providing Fraud Awareness Training To The Workforce / Info Graphic
Providing fraud awareness training to staff at all levels of an organization is a vital part of a comprehensive anti-fraud program. Our study shows that training employees, managers, and executives about the risks and costs of fraud can help reduce fraud losses and ensure frauds are caught more quickly. **43% of frauds were detected by a tip**. (Source)

FRAUD RESOURCES

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Fraud Risk Schemes Assessment Guide

Fraud Risk Management Scorecards

Other Tools

DEPARTMENT OF DEFENSE FRAUD DETECTION RESOURCES

General Fraud Indicators & Management Related Fraud Indicators

Fraud Red Flags & Indicators

Comprehensive List Of Fraud Indicators

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEE FRAUD

TD Bank Pleads Guilty To Money Laundering Conspiracy / Employees Accepted $57,000+ In Bribes / FINED $1.8 BILLION - October 10, 2024

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Customer Service Employee For Business Telephone System Provider & 2 Others Sentenced To Prison For $88 Million Fraud Scheme To Sell Pirated Software Licenses - July 26, 2024

3 individuals have been sentenced for participating in an international scheme involving the sale of tens of thousands of pirated business telephone system software licenses with a retail value of over $88 million.

Brad and Dusti Pearce conspired with Jason Hines to commit wire fraud in a scheme that involved generating and then selling unauthorized Avaya Direct International (ADI) software licenses. The ADI software licenses were used to unlock features and functionalities of a popular telephone system product called "IP Office" used by thousands of companies around the world. The ADI software licensing system has since been decommissioned.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

70 Current & Former New York City Housing Authority Employees Charged With $2 Million Bribery, Extortion And Contract Fraud Offenses - February 6, 2024

The defendants, all of whom were NYCHA employees during the time of the relevant conduct, demanded and received cash in exchange for NYCHA contracts by either requiring contractors to pay up front in order to be awarded the contracts or requiring payment after the contractor finished the work and needed a NYCHA employee to sign off on the completed job so the contractor could receive payment from NYCHA.

The defendants typically demanded approximately 10% to 20% of the contract value, between $500 and $2,000 depending on the size of the contract, but some defendants demanded even higher amounts. In total, these defendants demanded over $2 million in corrupt payments from contractors in exchange for awarding over $13 million worth of no-bid contracts. (Source)

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

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

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

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

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

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

University Financial Advisor Sentenced To Prison For $5.6 Million+ Wire Fraud Financial Aid Scheme (Over 15 Years - Involving 60+ Students) - August 30, 2023

As detailed in court documents and his plea agreement, from about 2006 until approximately 2021, Randolph Stanley and his co-conspirators engaged in a scheme to defraud the U.S. Department of Education. Stanley, was employed as a Financial Advisor at a University headquartered in Adelphi, Maryland. He and his co-conspirators recruited over 60 individuals (Student Participants) to apply for and enroll in post-graduate programs at more than eight academic institutions. Stanley and his co-conspirators told Student Participants that they would assist with the coursework for these programs, including completing assignments and participating in online classes on behalf of the Student Participants, in exchange for a fee.

As a result, the Student Participants fraudulently received credit for the courses, and in many cases, degrees from the Schools, without doing the necessary work.

Stanley also admitted that he and his co-conspirators directed the Student Participants to apply for federal student loans. Many of the Student Participant were not qualified for the programs to which they applied.

Student Participants, as well as Stanley himself, were awarded tuition, which went directly to the Schools and at least 60 Student Participants also received student loan refunds, which the Schools disbursed to Student Participants after collecting the tuition. Stanley, as the ringleader of the scheme, kept a portion of each of the students' loan refunds.

The Judge ordered that Stanley must pay restitution in the full amount of the victims' losses, which is at least $5,648,238, the outstanding balance on all federal student loans that Stanley obtained on behalf of himself and others as part of the scheme. (Source)

3 Bank Board Members Of Failed Bank Found Guilty Of Embezzling $31 Million From Bank / 16 Other Charged - August 8. 2023

William Mahon, George Kozdemba and Janice Weston were members of Washington Federal's Board of Directors. Weston also served as the bank's Senior Vice President and Compliance Officer.

Washington Federal was closed in 2017 after the Office of the Comptroller of the Currency determined that the bank was insolvent and had at least $66 million in nonperforming loans. A federal investigation led to criminal charges against 16 defendants, including charges against the bank's Chief Financial Officer, Treasurer, and other high-ranking employees, for conspiring to embezzle at least $31 million in bank funds. Eight defendants have pleaded guilty or entered into agreements to cooperate with the government. (Source)

5 Current And Former Police Officers Convicted In $3 Million+ COVID-19 Loan Scheme Involving 200 Individuals - April 6, 2023

Former Fulton County Sheriff's Office deputy Katrina Lawson has been found guilty of conspiracy to commit wire fraud, wire fraud, bank fraud, mail fraud, and money laundering in connection with a wide-ranging Paycheck Protection Program and Economic Injury Disaster Loan program small business loan scheme.

On August 11, 2020, agents from the U.S. Postal Inspection Service (USPIS) conducted a search at Alicia Quarterman's residence in Fayetteville, Georgia related to an ongoing narcotics trafficking investigation. Inspectors seized Quarterman's cell phone and a notebook during the search.

In the phone and notebook, law enforcement discovered evidence of a Paycheck Protection Program (PPP) and Economic Injury Disaster Loan (EIDL) program scheme masterminded by Lawson (Quarterman's distant relative and best friend). Lawson's cell phone was also seized later as a part of the investigation.

Lawson and Quarterman recruited several other people, who did not actually own registered businesses, to provide them with their personal and banking information. Once Lawson ultimately obtained that information, she completed fraudulent applications and submitted them to the Small Business Administration and banks for forgivable small business loans and grants.

Lawson was responsible for recruiting more than 200 individuals to participate in this PPP and EIDL fraud scheme. Three of the individuals she recruited were active sheriff's deputies and one was a former U.S. Army military policeman.

Lawson submitted PPP and EIDL applications seeking over $6 million in funds earmarked to save small businesses from the impacts of COVID-19. She and her co-conspirators ultimately stole more than $3 Million. Lawson used a portion of these funds to purchase a $74,492 Mercedes Benz, a $13,500 Kawasaki motorcycle, $9000 worth of liposuction, and several other expensive items. (Source)

President Of Building And Construction Trades Council Sentenced To Prison For Accepting $140,000+ In Bribes / 10 Other Union Officials Sentenced For Accepting Bribes And Illegal Payments - May 18, 2023

James Cahill was the President of the New York State Building and Construction Trades Council (NYS Trades Council), which represents over 200,000 unionized construction workers, a member of the Executive Council for the New York State American Federation of Labor and Congress of Industrial Organizations (NYS AFL-CIO), and formerly a union representative of the United Association of Journeymen and Apprentices of the Plumbing and Pipefitting Industry of the United States and Canada (UA).

From about October 2018 to October 2020, Cahill accepted approximately $44,500 in bribes from Employer-1, as well as other benefits, including home appliances and free labor on Cahill's vacation home.

Cahill acknowledged having previously accepted at least approximately $100,000 of additional bribes from Employer-1 in connection with Cahill's union positions. As the leader of the conspiracy, Cahill introduced Employer-1 to many of the other defendants, while advising Employer-1 that Employer-1 could reap the benefits of being associated with the unions without actually signing union agreements or employing union workers. (Source)

TRADE SECRET THEFT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

EMPLOYEES' WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

Former Bank President Sentenced To Prison For Role In $1 BILLION Fraud Scheme, Resulting In 500 Lost Jobs & Causing Bank To Cease Operations - September 6, 2023

Ashton Ryan was the President, CEO, and Chairman of the Board at First NBC Bank.

According to court documents and evidence presented at trial, Ryan and others conspired to defraud the Bank through a variety of schemes, including by disguising the true financial status of certain borrowers and their troubled loans, and concealing the true financial condition of the Bank from the Bank's Board, external auditors, and federal examiners.

As Ryan's fraud grew, it included several other bank employees and businesspeople. Several of the borrowers who conspired with Ryan, used the banks money to pay Ryani ndividually or fund Ryan's own businesses. Using bank money this way helped Ryanconceal his use of such money for his own benefit.

When the Bank's Board, external auditors, and FDIC examiners asked about loans to these borrowers, Ryan and his fellow fraudsters lied about the borrowers and their loans, hiding the truth about the deadbeat borrowers' inability to pay their debts without receiving new loans.

As a result, the balance on the borrowers' fraudulent loans continued to grow, resulting, ultimately, in the failure of the Bank in April 2017. This failure caused approximately $1 billion in loss to the FDIC and the loss of approximately 500 jobs.

Ryan was ordered to pay restitution totaling over $214 Million to the FDIC. (Source)

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

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

The funds were transferred to multiple cryptocurrency accounts controlled by unidentified third parties during the time HTSB was insured by the Federal Deposit Insurance Corporation (FDIC). The FDIC absorbed the $47.1 million loss. Hanes' fraudulent actions caused HTSB to fail and the bank investors to lose $9 million. (Source)

3 Bank Board Members Of Found Guilty Of Embezzling $31 Million From Bank / 16 Other Charged / Bank Collapsed - August 8. 2023

William Mahon, George Kozdemba and Janice Weston were members of Washington Federal's Board of Directors. Weston also served as the bank's Senior Vice President and Compliance Officer.

Washington Federal was closed in 2017 after the Office of the Comptroller of the Currency determined that the bank was insolvent and had at least $66 million in nonperforming loans.

A federal investigation led to criminal charges against 16 defendants, including charges against the bank's Chief Financial Officer, Treasurer, and other high-ranking employees, for conspiring to embezzle at least $31 million in bank funds. Eight defendants have pleaded guilty or entered into agreements to cooperate with the government. (Source)

Former Employee Admits To Participating In $17 Million Bank Fraud Scheme / Company Goes Out Of Business - April 17, 2024

A former employee (Nitin Vats) of a now-defunct New Jersey based marble and granite wholesaler, admitted his role in a scheme to defraud a bank in connection with a secured line of credit.

From March 2016 through March 2018, an owner and employees of Lotus Exim International Inc. (LEI), including Vats, conspired to obtain from the victim bank a $17 million line of credit by fraudulent means. The victim bank extended LEI the line of credit, believing it to have been secured in part by LEI's accounts receivable. In reality, the conspirators had fabricated and inflated many of the accounts receivable, ultimately leading to LEI defaulting on the line of credit.

To conceal the lack of sufficient collateral, Vats created fake email addresses on behalf of LEI's customers so that other LEI employees could pose as those customers and answer the victim bank's and outside auditor's inquiries about the accounts receivable.

The scheme involved numerous fraudulent accounts receivable where the outstanding balances were either inflated or entirely fabricated. The scheme caused the victim bank losses of approximately $17 million. (Source)

Bank Director Convicted For $1.4 Million Of Bank Fraud Causing Bank To Collapse - July 12, 2023

In 2009, Mendel Zilberberg (Bank Director) conspired with Aron Fried and others to obtain a fraudulent loan from Park Avenue Bank. Knowing that the conspirators would not be able to obtain the loan directly, the conspirators recruited a straw borrower (Straw Borrower) to make the loan application. The Straw Borrower applied for a $1.4 Million loan from the Bank on the basis of numerous lies directed by Zilberberg and his coconspirators.

Zilberberg used his privileged position at the bank to ensure that the loan was processed promptly.

Based on the false representations made to the Bank and Zilberberg's involvement in the loan approval process, the Bank issued a $1.4 Million loan to the Straw Borrower, which was quickly disbursed to the defendants through multiple bank accounts and transfers. In total, Zilberberg received more than approximately $500,000 of the loan proceeds. The remainder of the loan was split between Fried and another conspirator.

The Straw Borrower received nothing from the loan. The loan ultimately defaulted, resulting in a loss of over $1 million. (Source)

Former Vice President Of Discovery Tours Pleads Guilty To Embezzling $600,000 Causing Company To Cease Operations & File For Bankruptcy - June 15, 2022

Joseph Cipolletti was employed as Vice President of Discovery Tours, Inc., a business that offered educational trips for students. Cipolletti managed the organization's finances, general ledger entries, accounts payable and accounts receivable. Cipolletti also had signature authority on Discovery Tours' business bank accounts.

From June 2014 to May 2018, Cipolletti devised a scheme to defraud parents and other student trip purchasers by diverting payments intended for these trips to his own personal use on items such as home renovations and vehicles.

As a result of Cipolletti's actions and subsequent attempts to cover up the scheme, in May 2018, Discovery Tours abruptly ended operations and filed for bankruptcy.

Student trips to Washington, D.C. were canceled for dozens of schools across Ohio and more than 5,000 families lost the money they had previously paid for trip fees.

Cipolletti embezzled more than $600,000 from his place of business and made false entries in the general ledger. (Source)

Credit Union CEO Sentenced To Prison For Involvement In Fraud Scheme That Resulted In $10 Million In Losses, Forcing Credit Union To Close - April 5, 2022

Helen Godfrey-Smith's was employed by the Shreveport Federal Credit Union (SFCU) from 1983 to 2017, and during much of that time was employed as the Chief Executive Officer (CEO) of the SFCU.

In October 2016, the SFCU, through Godfrey-Smith, entered into an agreement with the United States Department of the Treasury to buy back certain securities that were part of the Department's Troubled Asset Relief Program (TARP). Godfrey-Smith signed and submitted to the United States Department of the Treasury an Officer's Certificate which certified that all conditions precedent to the closing had been satisfied.

In reality, SFCU had not met all conditions precedent to closing and had suffered a material adverse effect. Unbeknownst to the United States Department of the Treasury, the SFCU was in a financial crisis.

From 2015 through 2017, another individual who was the Chief Financial Officer (CFO) of SFCU had been falsifying reports. In addition, she was creating fictitious entries in the banks records to support the false reports.

This created the illusion that SFCU was profitable when, in fact, the bank was failing. The CFO embezzled approximately $1.5 million from the credit union.

By the time Godfrey-Smith signed the CFO's statement, she had become aware of deficiencies at the credit union.

Godfrey-Smith investigated and discovered that there were millions of dollars of fictitious entries on SFCU's general ledger, and the credit union's books were not balanced. But she failed to disclose this information to the United States Department of the Treasury and signed the false Officer's Statement.

In the Spring of 2017, the credit union failed. An investigation by revealed that SFCU had amassed in excess of $10 million in losses by December 2016. (Source)

Packaging Company Controller Sentenced To Prison For Stealing Funds Forcing Company Out Of Business (2021)

Victoria Mazur was employed as the Controller for Gateway Packaging Corporation, which was located in Export, PA.

From December 2012 until December 2017, she issued herself and her husband a total of approximately 189 fraudulent credit card refunds, totaling $195,063.80, through the company's point of sale terminal. Her thefts were so extensive, they caused the failure of the company, which is now out of business. In order to conceal her fraud, Mazur supplied the owners with false financial statements that understated the company's true sales figures. (Source)

Controller Of Oil & Gas Company Sentenced To Prison For Role in $65 Million Bank Fraud Scheme Over 21 Years / 275 Employees' Lost Jobs (2016)

In September 2020, Judith Avilez, the former Controller of Worley & Obetz, pleaded guilty to her role in a scheme that defrauded Fulton Bank of over $65 million. Avilez admitted that from 2016 through May 2018, she helped Worley & Obetz's CEO, Jeffrey Lyons, defraud Fulton Bank by creating fraudulent financial statements that grossly inflated accounts receivable for Worley & Obetz's largest customer, Giant Food. Worley & Obetz was an oil and gas company in Manheim, PA, that provided home heating oil, gasoline, diesel, and propane to its customers.

Lyons initiated the fraud shortly after he became CEO in 1999.

In order to make Worley & Obetz appear more profitable and himself appear successful as the CEO, Lyons asked the previous Worley & Obetz Controller, Karen Connelly, to falsify the company's financial statements to make it appear to have millions more in revenue and accounts receivable than it did.

Lyons and Connelly continued the fraud scheme from 2003 until 2016, when Connelly retired and Avilez became the Controller and joined the fraud. Avilez and Lyons continued the scheme in the same manner that Lyons and Connelly had. Each month, Avilez created false Worley & Obetz financial statements that Lyons presented to Fulton Bank in support of his request for additional loans or extensions on existing lines of credit. In total, Lyons, Connelly, and Avilez defrauded Fulton Bank out of $65,000,000 in loans.

After the scheme was discovered, Worley & Obetz and its related companies did not have the assets to repay the massive amount of Fulton loans Lyons had accumulated.

In June 2018, Worley & Obetz declared bankruptcy and notified its approximately 275 employees' that they no longer had jobs. After 72 years, the Obetz's family-owned company closed its doors forever.

The fraud Lyons committed with the help of Avilez and Connelly caused many families in the Manheim community to suffer financially and emotionally. Fulton Bank received some repayments from the bankruptcy proceedings but is still owed over $50,000,000. (Source)

Former Engineering Supervisor Costs Company $1 Billion In Shareholder Equity / 700 Employees' Lost Jobs (2011)

AMSC formed a partnership with Chinese wind turbine company Sinovel in 2010. In 2011, an Automation Engineering Supervisor at AMSC secretly downloaded AMSC source code and turned it over to Sinovell. Sinovel then used this same source code in its wind turbines.

2 Sinovel employees' and 1 AMSC employee were charged with stealing proprietary wind turbine technology from AMSC in order to produce their own turbines powered by stolen intellectual property.

Rather than pay AMSC for more than $800 million in products and services it had agreed to purchase, Sinovel instead hatched a scheme to brazenly steal AMSC's proprietary wind turbine technology, causing the loss of almost 700 jobs which accounted for more than half of its global workforce, and more than $1 billion in shareholder equity at AMSC. (Source)

EMPLOYEE EXTORTION

Former IT Employee Pleads Guilty To Stealing Confidential Data And Extorting Company For $2 Million In Ransom / He Also Publishes Misleading News Articles Costing Company $4 BILLION+ In Market Capitalization - February 2, 2023

Nickolas Sharp was employed by his company (Ubiquiti Networks) from August 2018 through April 1, 2021. Sharp was a Senior Developer who had administrative to credentials for company's Amazon Web Services (AWS) and GitHub servers.

Sharp pled guilty to multiple federal crimes in connection with a scheme he perpetrated to secretly steal gigabytes of confidential files from his technology company where he was employed.

While purportedly working to remediate the security breach for his company, that he caused, Sharp extorted the company for nearly $2 million for the return of the files and the identification of a remaining purported vulnerability.

Sharp subsequently re-victimized his employer by causing the publication of misleading news articles about the company's handling of the breach that he perpetrated, which were followed by the loss of over $4 billion in market capitalization.

Several days after the FBI executed the search warrant at Sharps's residence, Sharp caused false news stories to be published about the incident and his company's response to the Incident and related disclosures. In those stories, Sharp identified himself as an anonymous whistleblower within company, who had worked on remediating the Incident. Sharp falsely claimed that his company had been hacked by an unidentified perpetrator who maliciously acquired root administrator access to his company's AWS accounts.

Sharp in fact had taken the his company's data using credentials to which he had access in his role as his company AWS Cloud Administrator. Sharp used the data in a failed attempt to his company for $2 Million. (Source)

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

Information Technology Professional Pleads Guilty To Sabotaging Employer's Computer Network After Quitting Company - September 28, 2022

Casey Umetsu worked as an Information Technology Professional for a prominent Hawaii-based financial company between 2017 and 2019. In that role, Umetsu was responsible for administering the company's computer network and assisting other employees' with computer and technology problems.

Umetsu admitted that, shortly after severing all ties with the company, he accessed a website the company used to manage its internet domain. After using his former employer's credentials to access the company's configuration settings on that website, Umetsu made numerous changes, including purposefully misdirecting web and email traffic to computers unaffiliated with the company, thereby incapacitating the company's web presence and email. Umetsu then prolonged the outage for several days by taking a variety of steps to keep the company locked out of the website. Umetsu admitted he caused the damage as part of a scheme to convince the company it should hire him back at a higher salary. (Source)

IT Systems Administrator Receives Poor Bonus And Sabotages 2000 IT Servers / 17,000 Workstations - Cost Company $3 Million+ (2002)

A former system administrator that was employed by UBS PaineWebber, a financial services firm, infected the company's network with malicious code. He was apparently irate about a poor salary bonus he received of $32,000. He was expecting $50,000.

The malicious code he used is said to have cost UBS $3.1 million in recovery expenses and thousands of lost man hours.

The malicious code was executed through a logic bomb which is a program on a timer set to execute at predetermined date and time. The attack impaired trading, while impacting over 2,000 servers and 17,000 individual workstations in the home office and 370 branch offices. Some of the information was never fully restored.

After installing the malicious code, he quit his job. Following, he bought puts against UBS. If the stock price for UBS went down, because of the malicious code for example, he would profit from that purchase. (Source)

Employee Sentenced To Prison For Sabotaging Cisco's Network With Damages Costing $2.4 Million (2018)

Sudhish Ramesh admitted to intentionally accessing Cisco Systems' cloud infrastructure that was hosted by Amazon Web Services without Cisco's permission on September 24, 2018.

Ramesh worked for Cisco and resigned in approximately April 2018. During his unauthorized access, Ramesh admitted that he deployed a code from his Google Cloud Project account that resulted in the deletion of 456 virtual machines for Cisco's WebEx Teams application, which provided video meetings, video messaging, file sharing, and other collaboration tools. He further admitted that he acted recklessly in deploying the code, and consciously disregarded the substantial risk that his conduct could harm to Cisco.

As a result of Ramesh's conduct, over 16,000 WebEx Teams accounts were shut down for up to two weeks, and caused Cisco to spend approximately $1,400,000 in employee time to restore the damage to the application and refund over $1,000,000 to affected customers. No customer data was compromised as a result of the defendant's conduct. (Source)

Former Credit Union Employee Pleads Guilty To Unauthorized Access To Computer System After Termination & Sabotage Of 20+GB's Of Data/ Causing $10,000 In Damages (2021)
Juliana Barile was fired from her position as a part-time employee with a New York Credit Union on May 19, 2021.

Two days later, on May 21, 2021, Barile remotely accessed the Credit Union's file server and deleted more than 20,000 files and almost 3,500 directories, totaling approximately 21.3 gigabytes of data.

The deleted data included files related to mortgage loan applications and the Credit Union's anti-ransomware protection software. Barile also opened confidential files.

After she accessed the computer server without authorization and destroyed files, Barile sent text messages to a friend explaining that "I deleted their shared network documents," referring to the Credit Union's share drive. To date, the Credit Union has spent approximately $10,000 in remediation expenses for Barile's unauthorized intrusion and destruction of data. (Source)

Fired IT System Administrator Sabotages Railway Network - February 14, 2018
Christopher Grupe was suspended for 12 days back in December 2015 for insubordination while working for the Canadian Pacific Railway (CPR). When he returned the CPR had already decided they no longer wanted to work with Grupe and fired him. Grupe argued and got them to agree to let him resign. Little did CPR know, Grupe had no intention of going quietly.

As an IT System Administrator, Grupe had in his possession a work laptop, remote access authentication token, and access badge. Before returning these, he decided to sabotage the railway's computer network. Logging into the system using his still-active credentials, Grupe removed admin-level access from other accounts, deleted important files from the network, and changed passwords so other employees' could no longer gain access. He also deleted any logs showing what he had done.

The laptop was then returned, Grupe left, and all hell broke loose. Other CPR employees' couldn't log into the computer network and the system quickly stopped working. The fix involved rebooting the network and performing the equivalent of a factory reset to regain access.

Grupe may have been smirking to himself knowing what was going on, but CPR's management decided to find out exactly what happened. They called in computer forensic experts who found the evidence needed to prosecute Grupe. Grupe was found guilty of carrying out the network sabotage and handed a 366 day prison term. (Source)

IT Systems Administrator Sentenced To Prison For Hacking Computer Systems Of His Former Employer - Causing Company To Go Out Of Business (2010)

Dariusz Prugar worked as a IT Systems Administrator for an Internet Service Provider (Pa Online) until June 2010. But after a series of personal issues, he was let go.

Prugar logged into PA Online's network, using his old username and password. With his network privileges he was able to install backdoors and retrieve code that he had been working on while employed at the ISP.

Prugar tried to cover his tracks, running a script that deleted logs, but this caused the ISP's systems to crash, impacting 500 businesses and over 5,000 residential customers of PA Online, causing them to lose access to the internet and their email accounts.

According to court documents, that could have had some pretty serious consequences: "Some of the customers were involved in the transportation of hazardous materials as well as the online distribution of pharmaceuticals."

Unaware that Prugar was responsible for the damage, PA Online contacted their former employee requesting his help. However, when Prugar requested the rights to software and scripts he had created while working at the firm in lieu of payment. Pa Online got suspicious and called in the FBI.

A third-party contractor was hired to fix the problem, but the damage to PA Online's reputation was done and the ISP lost multiple clients.

Prugar ultimately pleaded guilty to computer hacking and wire fraud charges, and received a two year prison sentence alongside a $26,000 fine.

And PA Online? Well, they went out of business in October 2015. (Source)

IT Administrator Sentenced To Prison For Attempting Computer Sabotage On 70 Company Servers / Feared He Was Going To Be Laid Off (2005)

Yung-Hsun Lin was a former Unix System Administrator at Medco Health Solutions Inc.'s Fair Lawn, N.J. He pleaded guilty in federal court to attempting to sabotage critical data, including individual prescription drug data, on more than 70 servers.

Lin was one of several systems administrators at Medco who feared they would get laid off when their company was being spun off from drug maker Merck & Co. in 2003, according to a statement released by federal law enforcement authorities. Apparently angered by the prospect of losing his job, Lin on Oct. 2, 2003, created a "logic bomb" by modifying existing computer code and inserting new code into Medco's servers.

The bomb was originally set to go off on April 23, 2004, on Lin's birthday. When it failed to deploy because of a programming error, Lin reset the logic bomb to deploy on April 23, 2005, despite the fact that he had not been laid off as feared. The bomb was discovered and neutralized in early January 2005, after it was discovered by a Medco computer systems administrator investigating a system error.

Had it gone off as scheduled, the malicious code would have wiped out data stored on 70 servers. Among the databases that would have been affected was a critical one that maintained patient-specific drug interaction information that pharmacists use to determine whether conflicts exist among an individual's prescribed drugs. Also affected would have been information on clinical analyses, rebate applications, billing, new prescription call-ins from doctors, coverage determination applications and employee payroll data. (Source)

Chicago Airport Contractor Employee Sets Fire To FAA Telecommunications Infrastructure System - September 26, 2014

In the early morning hours of September 26, 2014, the Federal Aviation Administration's (FAA) Chicago Air Route Traffic Control Center (ARTCC) declared ATC Zero after an employee of the Harris Corporation deliberately set a fire in a critical area of the facility. The fire destroyed the Center's FAA Telecommunications Infrastructure (FTI) system – the telecommunications structure that enables communication between controllers and aircraft and the processing of flight plan data.

Over the course of 17 days, FAA technical teams worked 24 hours a day alongside the Harris Corporation to completely rebuild and replace the destroyed communications equipment. They restored, installed and tested more than 20 racks of equipment, 835 telecommunications circuits and more than 10 miles of cables. (Source)

Lottery Official Tried To Rig $14 Million+ Jackpot By Inserting Software Code Into Computer That Picked Numbers - Largest Lottery Fraud In U.S. History - 2010

This incident happened in 2010, but the articles on the links below are worth reading, and are great examples of all the indicators that were ignored.

Eddie Tipton was a Lottery Official in Iowa. Tipton had been working for the Des Moines based Multi-State Lottery Association (MSLA) since 2003, and was promoted to the Information Security Director in 2013.

Tipton was first convicted in October 2015 of rigging a $14.3 Million drawing of the MSLA lottery game Hot Lotto. Tipton never got his hands on the winning total, but was sentenced to prison. Tipton was released on parole in July 2022.

Tipton and his brother Tommy Tipton were subsequently accused of rigging other lottery drawings, dating back as far as 2005.

Based on forensic examination of the random number generator that had been used in a 2007 Wisconsin lottery incident, investigators discovered that Eddie Tipton programmed a lottery random number generator to produce special results if the lottery numbers were drawn on certain days of the year.

That software code was replicated on as many as 17 state lottery systems, as the MSLA random-number software was designed by Tipton. For nearly a decade, it allowed Tipton to rig the drawings for games played on three dates each year: May 27, Nov. 23 and Dec. 29.

Tipton ultimately confessed to rigging other lottery drawings in Colorado, Wisconsin, Kansas and Oklahoma.

UNDERAPPRECIATED / OVERWORKED / NO OVERSIGHT

Eddie Tipton was making almost $100,000 a year. But he felt underappreciated and overworked at the time he wrote the code to hack into the national lottery system.

He was working 50- to 60-hour weeks and often was in the office until 11 p.m. His managers expected him to take on far more roles than were practical, he complained.

Tipton Stated: "I wrote software. I worked on Web pages. I did network security. I did firewalls," he said in his confession. "And then I did my regular auditing job on top of all that. They just found no limits to what they wanted to make me do. It even got to the point where the word 'slave' was used."

Nobody at the MSLA oversaw his complete body of work, and few people truly cared about security, he said. That lack of oversight allowed Tipton to write, install and use his secret code without discovery.
Video Complete Story Indicators Overlooked / Ignored

DESTRUCTION OF EMPLOYERS PROPERTY BY EMPLOYEES

Bank President Sets Fire To Bank To Conceal $11 Million Fraud Scheme - February 22, 2021

On May 11, 2019, while Anita Moody was President of Enloe State Bank in Cooper, Texas, the bank suffered a fire that investigators later determined to be arson. The fire was contained to the bank's boardroom however the entire bank suffered smoke damage.

Investigation revealed that several files had been purposefully stacked on the boardroom table, all of which were burned in the fire. The bank was scheduled for a review by the Texas Department of Banking the very next day.

The investigation revealed that Moody had created false nominee loans in the names of several people, including actual bank customers. Moody eventually admitted to setting the fire in the boardroom to conceal her criminal activity concerning the false loans.

She also admitted to using the fraudulently obtained money to fund her boyfriend's business, other businesses of friends, and her own lifestyle. The fraudulent activity, which began in 2012, resulted in a loss to the bank of approximately $11 million dollars. (Source)

Fired Hotel Employee Charged For Arson At Hotel That Displaced 400 Occupants - June 29, 2023

Ramona Cook has been indicted on an arson charge and accused of setting fires at a hotel after being fired.

On Dec. 22, 2022, Cook maliciously damaged the Marriott St. Louis Airport Hotel.

Cook was fired for being intoxicated at work. She returned shortly after being escorted out of the hotel by police and set multiple fires in the hotel, displacing the occupants of more than 400 rooms. (Source)

WORKPLACE VIOLENCE

Anesthesiologist Working At Surgical Center Sentenced To 190 Years In Prison For Tampering With IV Bags / Resulting In Cardiac Emergencies & Death - November 20, 2024

Raynaldo Ortiz, a Dallas, Texas anesthesiologist was convicted for injecting dangerous drugs into patient IV bags, leading to one death and numerous cardiac emergencies.

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

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

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

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

Spectrum Cable Company Ordered By Judge To Pay $1.1 BILLION After Customer Was Murdered By Spectrum Employee - September 20, 2022

A Texas judge ruled that Charter Spectrum must pay about $1.1 billion in damages to the estate and family members of 83 year old Betty Thomas, who was murdered by a cable repairman inside her home in 2019.

A jury initially awarded more than $7 billion in damages in July, but the judge lowered that number to roughly $1.1 Billion.

Roy Holden, the former employee who murdered Thomas, performed a service call at her home in December 2019. The next day, while off-duty, he went back to her house and stole her credit cards as he was fixing her fax machine, then stabbed her to death before going on a spending spree with the stolen cards.

The attorneys also argued that Charter Spectrum hired Holden without reviewing his work history and ignored red flags during his employment. (Source) (Source)

Former Nurse Charged With Murder Of 2 Patients At Hospital, Nearly Killing 3rd By Administering Lethal Doses Of Insulin - October 26, 2022

Jonathan Hayes, a 47-year-old former Nurse at Atrium Health Wake Forest Baptist Medical Center in Winston-Salem, North Carolina, has been charged with 2 counts of murder and 1 count of attempted murder.

O'Neill said that on March 21, a team of investigators at the hospital presented him with information that Hayes may have administered a lethal dose of insulin to one patient and indicated there may be other victims.

The 1 count of murder against Hayes is related to the death of 61 year old Jen Crawford. Hayes administered a lethal dose of insulin to Crawford on Jan. 5. She died three days later.

The 2 count of murder is in connection with the death of 62-year-old Vickie Lingerfelt, who was administered a lethal dose of insulin on Jan. 22. She died on Jan. 27.

Hayes is also charged with administering a near-lethal dose of insulin to 62-year-old Pamela Little on Dec. 1, 2021. Little survived and Hayes faces one count of attempted murder.

Hayes was terminated from the hospital in March 2022, and he was arrested In October 2022. (Source)

Hospital Nurse Alleged Killer Of 7 Babies / 15 Attempted Murders - October 13, 2022

A neonatal nurse in the U.K. who allegedly murdered 7 babies and attempted to kill 10 more wrote notes reading, "I don't deserve to live," "I killed them on purpose because I'm not good enough to care for them. I am a horrible evil person."

Lucy Letby, 32, who worked in the Neonatal Unit of the Countess of Chester Hospital, left handwritten notes in her home that police found when they searched it in 2018, prosecutor Nick Johnson stated during her trial in October 2022.

Johnson argued that Letby was a constant, malevolent presence in the neonatal unit. Of the babies Letby allegedly murdered or attempted to murder between 2015 and 2016, the prosecution said she injected some with insulin or milk, while another she injected with air. She allegedly attempted to kill one baby three times.

Johnson told jurors the hospital had been marked by a significant rise in the number of babies who were dying and in the number of serious catastrophic collapses" after January 2015, before which he said its rates of infant mortality were comparable to other busy hospitals.

Investigators found Letby was the "common denominator," and that the infant deaths aligned with her shifting work hours.

Letby pleaded not guilty to seven counts of murder and 15 counts of attempted murder. Her trial is slated to last for up to six months. (Source)

Veterans Affairs Medical Center Nursing Assistant Sentenced To 7 Consecutive Life Sentences For Murdering 7 Veterans - May 11, 2021

Reta Mays was sentenced to 7 consecutive life sentences, one for each murder, and an additional 240 months for the eight victim. Mays pleaded guilty in July 2020 to 7 counts of second-degree murder in the deaths of the veterans. She pleaded guilty to one count of assault with intent to commit murder involving the death of another veteran.

Mays was employed as a nursing assistant at the Veterans Affairs Medical Center (VAMC) in Clarksburg, West Virginia. She was working the night shift during the same period of time that the veterans in her care died of hypoglycemia while being treated at the hospital. Nursing assistants at the VAMC are not qualified or authorized to administer any medication to patients, including insulin. Mays would sit one-on-one with patients. She admitted to administering insulin to several patients with the intent to cause their deaths.

This investigation, which began in June 2018, involved more than 300 interviews; the review of thousands of pages of medical records and charts; the review of phone, social media, and computer records; countless hours of consulting with some of the most respected forensic experts and endocrinologists; the exhumation of some of the victims; and the review of hospital staff and visitor records to assess their potential interactions with the victims. (Source)

Indianapolis FedEx Shooter That Killed 8 People Was Former FedEx Employee With Mental Health Problems - April 20, 2021

Police say the 19 year old Indianapolis man who fatally shot 8 people at a southwest side FedEx Ground facility in April had planned the attack for at least nine months.

In a press conference, local and federal officials said the shooting was "an act of suicidal murder" in which Bandon Scott Hole decided to kill himself "in a way he believed would demonstrate his masculinity and capability while fulfilling a final desire to experience killing people."

Hole worked at the FedEx facility between August and October 2020. Police believe he targeted his former workplace not because he was trying to right a perceived injustice, but because he was familiar with the "pattern of activity" at the site.

FBI Indianapolis Special Agent in Charge Paul Keenan said Hole's focus on proving his masculinity was partially connected to a failed attempt to live on his own, which ended with him moving back into his old house.

Investigators also learned Hole aspired to join the military. Authorities said he had been eating MREs, or meals ready-to-eat, like those consumed by members of the armed forces.

Keenan also said Hole had suicidal thoughts that "occurred almost daily" in the months leading up to the shooting. The police had previously responded to Hole's home in March 2020 on a mental health check.

Hole was put under an immediate detention at a local hospital and a gun he had recently bought was confiscated. Hole would later buy more guns and use them in the FedEx shooting, according to police. (Source)

Xerox Employee Receives Life In Prison For Credit Union Robbery And Murder - September 22, 2020

On August 12, 2003, Richard Wilbern walked into Xerox Federal Credit Union, located on the Xerox Corporation campus, and committed robbery and murder. Wilbern was not caught until 2016 for robbery and murder, and was sentenced this week to life in prison.

Richard Wilbern walked into Xerox Federal Credit Union (XFCU) and was wearing a dark blue nylon jacket with the letters FBI written in yellow on the back of the jacket, sunglasses and a poorly fitting wig. Wilbern was also carrying a large briefcase, a green and gray-colored umbrella and had what appeared to be a United States Marshals badge hanging on a chain around his neck.

Wilbern was employed by Xerox between September 1996 and February 23, 2001 as which time he was terminated for repeated employment related infractions. In 2001, Wilbern filed a lawsuit against Xerox alleging that the company unlawfully discriminated against him with respect to the terms and conditions of his employment, subjected him to a hostile work environment, failed to hire him for a position for which he applied because of his race, and retaliated against him for complaining about Xerox's discriminatory treatment. Wilbern also maintained a checking and savings accounts at the Xerox Federal Credit Union. Evidence at trial demonstrated that Wilbern was in significant financial distress from roughly 2000 – 2003, including filing for bankruptcy.

In March 2016, a press conference was held to seek new leads in the investigation. Details of the crime were released as well as photographs of Wilbern committing the robbery. Anyone with information was asked to call a dedicated hotline.

On March 27, 2016, a concerned citizen contacted the Federal Bureau of Investigation and indicated that the person who committed the crime was likely a former Xerox employee named Richard Wilbern.

The citizen indicated that the defendant worked for Xerox prior to the robbery but had been fired. The citizen also stated that they recognized Wilbern's face from the photos.

In July 20016, FBI agents met with Wilbern regarding a complaint he had made to the FBI regarding an alleged real estate scam. During one of their meetings, agents obtained a DNA sample from Wilbern after he licked and sealed an envelope. That envelope was sent to OCME, and after comparing the DNA profile from the envelope to the DNA profile previously developed from the umbrella, determined there was a positive match. (Source)

Florida Best Buy Driver Murders 75 Year Old Woman While Delivering Her Appliances - Lawyers Said The Murder Was Preventable If Best Buy Had Better Screened Employees' - September 30, 2019

A Boca Raton family has filed a wrongful death lawsuit against Best Buy. This comes after allegations a delivery man for the company killed a 75-year-old woman while delivering appliances.

The family of 75 year old Evelyn Udell has filed a wrongful death lawsuit to hold Best Buy, two delivery contractors and the two deliverymen, accountable for her death.

Lawyers say the fatal attack was preventable if the companies had further screened their employees'.

On August 19th, police say Jorge Lachazo and another man were delivering a washer and dryer the Udells had bought from Best Buy.

Police say Lachazo beat Udell with a mallet, poured acetone on her body and set her on fire. She died the next day. Lachazo was arrested and is charged with murder.

According to the lawsuit, Best buy stores did nothing to investigate, supervise, or oversee the personnel used to perform these services on their behalf. Worse, it did nothing to advise, inform, or warn Mrs. Udell that the delivery and installation services had been delegated to a third-party.

Lawyers are also calling for sweeping changes to how businesses screen workers who have to go inside a customers' home. (Source)

INSIDERS WHO STOLE TRADE SECRETS / RESEARCH FOR CHINA / OR HAD TIES TO CHINA

CTTP = China Thousand Talents Plan

- NIH Reveals That 500+ U.S. Scientist's Are Under Investigation For Being Compromised By China And Other Foreign Powers
- U.S. Petroleum Company Scientist STP For $1 Billion Theft Of Trade Secrets - Was Starting New Job In China
- Cleveland Clinic Doctor Arrested For $3.6 Million Grant Funding Fraud Scheme Involving CTTP
- Hospital Researcher STP For Conspiring To Steal Trade Secrets And Sell Them in China With Help Of Husband
- Employee Of Research Institute Pleads Guilty To Steal Trade Secrets To Sell Them In China
- Raytheon Engineer STP For Exporting Sensitive Military Technology To China
- GE Power & Water Employee Charged With Stealing Turbine Technologies Trade Secrets Using Steganography For Data Exfiltration To Benefit People's Republic of China
- CIA Officer Charged With Espionage Over 10 Years Involving People's Republic of China
- Massachusetts Institute of Technology (MIT) Professor Charged With Grant Fraud Involving CTTP
- Employee At Los Alamos National Laboratory Receives Probation For Making False Statements About Being Employed By CTTP
- Texas A&M University Professor Arrested For Concealing His Association With CTTP
- West Virginia University Professor STP For Fraud And Participation In CTTP
- Harvard University Professor Charged With Receiving Financial Support From CTTP
- Visiting Chinese Professor At University of Texas Pleads Guilty To Lying To FBI About Stealing American Technology
- Researcher Who Worked At Nationwide Children's Hospital's Research Institute For 10 Years, Pleads Guilty To Stealing Scientific Trade Secrets To Sell To China
- U.S. University Researcher Charged With Illegally Using $4.1 Million In U.S. Grant Funds To Develop Scientific Expertise For China
- U.S. University Researcher Charged With VISA Fraud And Concealed Her Membership In Chinese Military
- Chinese Citizen Who Worked For U.S. Company Convicted Of Economic Espionage, Theft Of Trade Secrets To Start New Business In China
- Tennessee University Researcher Who Was Receiving Funding From NASA Arrested For Hiding Affiliation With A Chinese University
- Engineers Found Guilty Of Stealing Micron Secrets For China
- Corning Employee Accused Of Theft Of Trade Secrets To Help Start New Business In China
- Husband And Wife Scientists Working For American Pharmaceutical Company, Plead Guilty To Illegally Importing Potentially Toxic Lab Chemicals And Illegally Forwarding Confidential Vaccine Research to China
- Former Coca-Cola Company Chemist Sentenced To Prison For Stealing Trade Secrets To Setup New Business In China
- Former Scientist Convicted For Role With Sister To Steal Trade Secrets From GlaxoSmithKline Worth $10 BILLION To Setup Business In China
- University Of Kansas Researcher Convicted For Hiding Ties To Chinese Government
- Former Employee (Chinese National) Sentenced To Prison For Conspiring To Steal Trade Secret From U.S. Company
- Federal Indictment Charges People's Republic Of China Telecommunications Company With Conspiring With Former Motorola Solutions Employees' To Steal Technology

- Former U.S. Navy Sailor Sentenced To Prison For Selling Export Controlled Military Equipment To China With Help Of Husband Who Was Also In Navy
- Former Broadcom Engineer Charged With Theft Of Trade Secrets - Provided Them To His New Employer A China Startup Company

SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

Produced By: National Insider Threat Special Interest Group / Insider Threat Defense Group

The websites listed below are updated daily and monthly with the latest incidents.
There is NO REGISTRATION required to download the reports.

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present / Updated Daily

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**6,600+ 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)

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. Download Report

Why Insider Threats Remain An Unresolved Cybersecurity Challenge
Produced By: IntroSecurity: NITSIG - ITDG / June 2025
The report was developed in collaboration with IntroSecurity and the NITSIG. It provides a practical and real world approach to Insider Risk Management (IRM), based off of research of actual Insider Threat incidents and the maturity levels of IRM Programs (IRMP's)

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

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

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

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

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

WORKPLACE VIOLENCE (WPV) INSIDER THREAT INCIDENTS E-MAGAZINE
This e-magazine contains WPV incidents that have occurred at organizations of all different types and sizes.

View On The Link Below Or Download The Flipboard App To View On Your Mobile Device
https://flipboard.com/@cybercops911/insider-threat-workplace-violence-incidents-e-magazine-last-update-8-1-22-r8avhdlcz

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

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS
https://www.nationalinsiderthreatsig.org/crticial-infrastructure-insider-threats.html

National Insider Threat Special Interest Group (NITSIG)

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

NITSIG Overview

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

NITSIG Membership

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

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

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

NITSIG Meetings

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

NITSIG IRM Resources

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

NITSIG LinkedIn Group

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

NITSIG Advisory Board

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

https://www.nationalinsiderthreatsig.org/aboutnitsig.html

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

INSIDER THREAT DEFENSE GROUP

INSIDER RISK MANAGEMENT PROGRAM EXPERTS
TRAINING & CONSULTING SERVICES

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

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

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

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

IRM PROGRAM TRAINING & CONSULTING SERVICES OFFERED

Conducted Via Classroom / Onsite / Web Based

TRAINING

- ✓ Executive Management & Stakeholder Briefings For IRM
- ✓ IRM Program Training Course & Workshop / Table Top Exercises For C-Suite, Insider Risk Program Manager / Working Group
- ✓ IRM Program Evaluation & Optimization Training Course (Develop, Management, Enhance)
- ✓ Insider Threat Investigations & Analysis Training Course With Legal Guidance From Attorney
- ✓ Insider Threat Awareness Training For Employees'

CONSULTING SERVICES

- ✓ Insider Risk - Threat Vulnerability Assessments
- ✓ IRM Program Maturity Evaluation, Gap Analysis & Strategic Planning Guidance
- ✓ Insider Threat Detection Tool Gap Analysis & Pre-Purchasing Guidance / Solutions
- ✓ Data Exfiltration / Red Team Assessment (Executing The Malicious Insiders Playbook Of Tactics)
- ✓ Technical Surveillance Counter-Measures Inspections (Covert Audio / Video Device Detection)
- ✓ Employee Continuous Monitoring & Reporting Services (External Data Sources)
- ✓ Customized IRM Consulting Services For Our Clients

STUDENT / CLIENT SATISFACTION

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

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

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

The ITDG Has Provided IRM Program Training / Consulting Services To An Impressive List Of 700+ Clients:

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

Additional Background Information On ITDG

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

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

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

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Risk Management Program Training Course Instructor / Consultant
Insider Threat Investigations & Analysis Training Course Instructor / Analyst
Insider Risk / Threat Vulnerability Assessor
561-809-6800
jimhenderson@insiderthreatdefensegroup.com
www.insiderthreatdefensegroup.com
LinkedIn ITDG Company Profile
Follow Us On Twitter / X: @InsiderThreatDG