INSIDER THREAT INCIDENTS REPORT
FOR
February 2024

Produced By

National Insider Threat Special Interest Group
U.S. Insider Risk Management Center Of Excellence
Insider Threat Defense Group

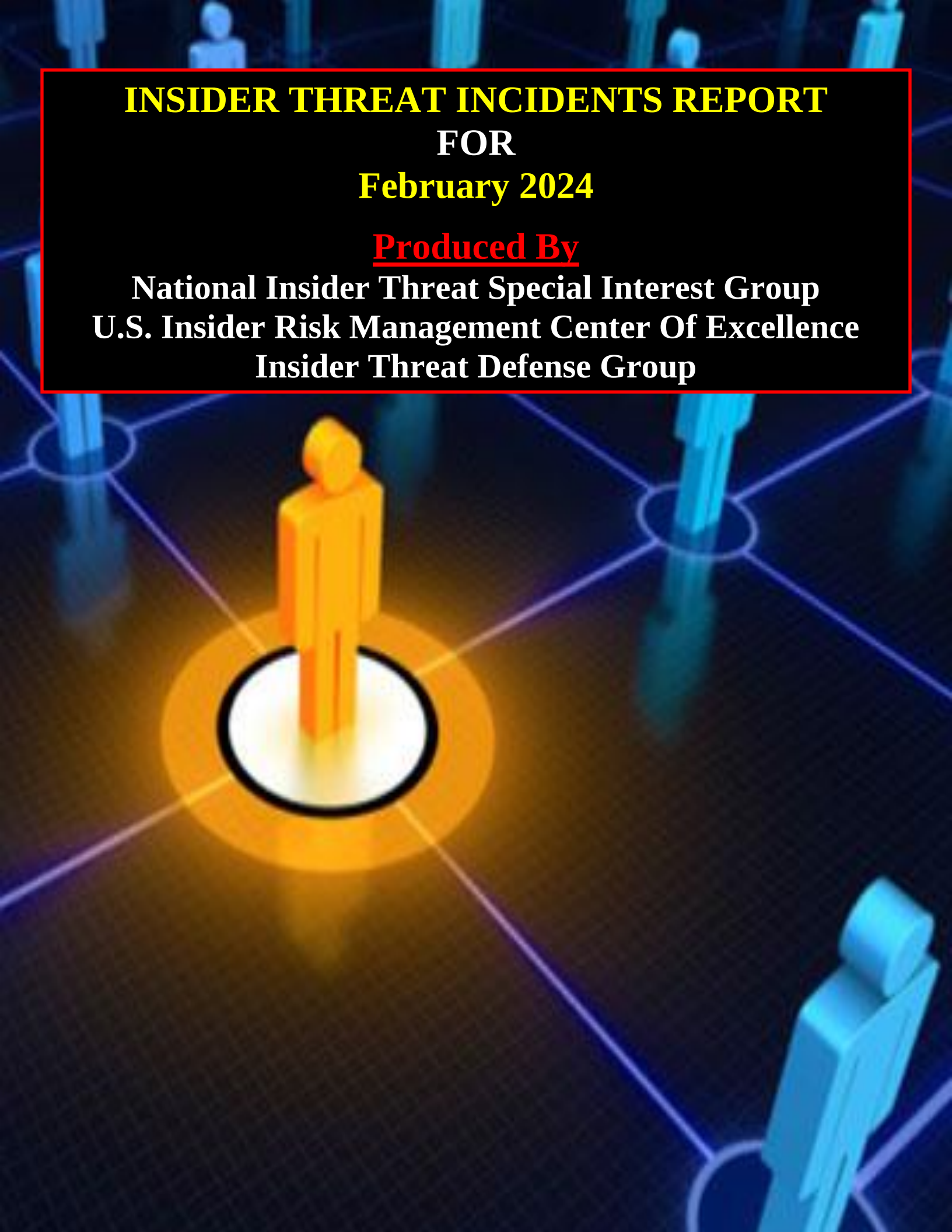


TABLE OF CONTENTS

INSIDER THREAT INCIDENTS

A Very Costly And Damaging Problem

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

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for 15+ years. This research has evaluated and analyzed over **5,000+** 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. Over the years there has been a drastic increase in financial fraud and embezzlement committed by employees'.

According to the Association of Certified Fraud Examiners 2022 Report to the Nations, organizations with less than 100 employees' suffered larger median losses than those of larger companies.

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 shows.

These monthly reports are recognized and used by Insider Risk Program Managers working for major corporations, as a **TRUSTED SOURCE** for education to gain support from CEO's, C-Suite, Key Stakeholders and Supervisors for detecting and mitigating Insider Threats. The incidents listed on pages **4 to 16** of this report provide the justification, return on investment and funding needed for developing, managing or optimizing an Insider Risk Management 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 FEBRUARY 2024

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

Member Of European Parliament Working As Undercover Russian Spy - February 4, 2024

Lawmakers in Europe have been shaken by allegations that Tatjana Ždanoka, a Latvian member of the European Parliament, has been working undercover as a Russian spy.

Since at least 2003, Ždanoka worked to arrange in-person meetings with her Russian intelligence contacts, from Moscow to Brussels, according to a joint investigation. The investigation cites emails and other correspondence, and alleges that Ždanoka also requested funding from the intelligence officers, and shared draft initiatives and press releases with them on several occasions.

The European Parliament has opened an investigation into the matter and lawmakers in Latvia are warning that there are other Russian spies in their ranks. (Source)

U.S. GOVERNMENT

U.S. Postal Service Employee Admits To Receiving $156,000+ Of Disability Fraud - January 30, 2024

Pamela VanSyckle worked for the U.S. Postal Service as a rural carrier.

In September 2020, VanSyckle signed and filed a claim form alleging that she sustained an injury at work. Thereafter, she signed and filed multiple federal claim forms alleging that she had not worked or had outside employment for extended periods of time. Based on the submission of those claims, VanSyckle received $156,872 in disability payments from the federal government.

During the time in which she received disability benefits, VanSyckle was in fact working as the owner and operator of a travel agency. While alleging in her claim forms that she was neither self-employed nor involved in any business enterprise, VanSyckle performed a variety of services for the travel agency including sales, marketing, and financial operations. (Source)

Former Puerto Rico Legislative Assistant Sentenced To Prison For Paycheck / Kickback Fraud Scheme - February 24, 2024

A former legislative assistant to a member of the Puerto Rico House of Representatives was sentenced to three years and one month in prison for engaging in a scheme to accept a fraudulently inflated government salary in exchange for providing kickbacks to a legislator and the legislator's family members.

From early 2013 until July 2020, Frances Acevedo-Ceballos served as a Legislative Assistant for María Milagros Charbonier-Laureano, a member of the Puerto Rico House of Representatives.

In early 2017, Charbonier-Laureano inflated Acevedo-Ceballos' salary from $800 on a bi-weekly, after-tax basis to over $2,100. Acevedo-Ceballos' bi-weekly, net government salary further increased to between $2,700 and $2,900 from the middle of 2017 until June 2020. Out of every inflated paycheck, it was agreed that Acevedo-Ceballos would keep a portion and pay kickbacks ranging between $1,000 and $1,500 to Charbonier-Laureano, Charbonier-Laureano's husband, Orlando Montes-Rivera, and Charbonier-Laureano's son, throughout the course of the scheme. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Former CIA Employee Sentenced To Prison For WikiLeaks Disclosures Of Classified Information / Substantial Possession Of Child Pornographic Materials - February 1, 2024

Joshua Schulte's theft is the largest data breach in the history of the CIA, and his transmission of that stolen information to WikiLeaks is one of the largest unauthorized disclosures of classified information in the history of the U.S. (Source)

Navy Chief Facing Charges For Passing Classified Information To A Foreign Government - February 21, 2024

Chief Petty Officer Fire Control Man Bryce Pedicini, a sailor assigned to a guided-missile destroyer based in Japan, has been charged with espionage and passing classified information to a foreign government contact.

Pedicini has been held in pre-trial confinement since May, according to Navy records.

The Navy is accusing Pedicini of smuggling classified information from secure spaces and giving them to an employee of an unspecified foreign government between late November 2022 to February 2023 in Hampton Roads, Va. The type of information Pedicini is accused of sharing was unclear from the charging documents, which also allege that he attempted to pass on photos, including those of a computer screen designated to handle secret information, to a foreign national while in Yokosuka, Japan.

The Chief is also accused of delivering similar classified information to a foreign contact seven other times, with the most recent alleged occurrence taking place on May 17, 2023 in Yokosuka, Japan.

Prosecutors also allege he failed to report a foreign contact in Yokosuka in April, and that he failed to report solicitation of classified information by an unauthorized person. Charge Sheet

Pedicini is also accused of taking a personal electronic device into a secure room aboard Barge APL-67 in Yokosuka in May, according to his charge sheet. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

U.S. Border Patrol Agent Pleads Guilty To Smuggling Immigrants And Drugs Into U.S. & Receiving Bribes - February 1, 2024

Former U.S. Border Patrol Agent Hector Hernandez pleaded guilty that he used his official position to smuggle unauthorized immigrants and illegal drugs across the border in exchange for money.

Hernandez admitted to using his official position to open border fences and allowing undocumented immigrants and controlled substances to enter the United States from Mexico. Hernandez also admitted to moving the drugs from the Southern District of California to other locations within the United States.

Hernandez admitted to taking Mexico-based smugglers on a tour of the US/Mexico border, identifying the best locations to sneak unauthorized immigrants into the United States, and sharing the locations of monitoring devices and cameras near the border to help them evade detection.

Hernandez also admitted to opening restricted border fences on at least five occasions and allowing immigrants to enter the United States for cash payments of $5,000 each time.

After Hernandez was arrested, agents searched his residence and found close to $140,000 in cash and 9 grams of cocaine. By Hernandez's own admission, at least $110,000 of the seized cash represented proceeds from narcotics trafficking and bribery. (Source)

4 Massachusetts State Troopers, 2 Others Arrested For Taking Bribes To Falsify Driver License Documentation - January 30, 2023

Two current and two former Massachusetts State Police (MSP) troopers are among six charged in a 74-count indictment in connection with an alleged conspiracy to falsify records and give passing scores to certain Commercial Driver's License (CDL) applicants, including individuals who had failed or did not take the CDL skills test, in exchange for bribes.

According to the charging document, between in on or about May 2019 and January 2023, Gary Cederquist, Calvin Butner, Perry Mendes, Joel Rogers and others conspired to give preferential treatment to at least 17 CDL applicants by agreeing to give passing scores on their skills tests whether or not they actually passed, using the code word "golden" to identify these applicants who received special treatment.

Cederquist accepted additional bribes in exchange for using his official position as the Sergeant in charge of MSP's CDL Unit to give preferential treatment to certain CDL applicants including, but also a $750 granite post and mailbox; a new driveway valued at over $10,000; and a snow blower valued at nearly $2,000.

The indictment alleges that Cederquist described one such applicant as "horrible," and "brain dead," but gave him a passing score anyway in exchange for the snow blower. (Source)

FBI Agent Charged With Theft Of Government Property & Money - Property When Conducting Search Warrants - January 31, 2024

Nicholas Williams has been an FBI Special Agent in the Houston Field Office since 2019. He allegedly served in both the criminal violent gang and counterterrorism squads.

The charges allege that from March 2022 to July 2023, Williams took money or property from multiple residences while executing search warrants as an FBI special agent and then allegedly converted the money or property to his personal use.

Williams also stole multiple cell phones which were FBI property and provided false statements with regard to several fraudulent charges on his government-issued credit card, according to the indictment. (Source)

STATE / CITY GOVERNMENTS / MAYORS

No Incidents To Report

SCHOOL SYSTEMS / UNIVERSITIES

Former Public University Administrator Sentenced To Prison For Diverting $1.5+ Million In Student Tuition Payments To Herself For Gambling, Home Improvements, Etc. - February 16, 2024

Sandra Le pleaded guilty on November 9, 2023, to three counts of wire fraud, in violation of 18 U.S.C. § 1343.

Le was the Academic Program Officer for the University of California, San Francisco (UCSF) School of Nursing's Post-Master's and Special Studies Certificate Programs.

Le abused her position by directing students in those programs to have their tuition checks made out to her, or to a merchandiser she purchased from, or to leave the checks' payee line blank so she could then make out the checks to herself or her associates. She then deposited the checks into her personal bank accounts, including joint bank accounts that she shared with associates, and used the funds to pay for luxury items from that merchandiser. She also used the funds for gambling, home improvement, and other personal expenses. Le disguised and concealed her misconduct by generating false records of payments and student enrollment for her supervisors at the university. The investigation into her conduct revealed that Le diverted almost 300 such checks from November 2013 through March 2019, totaling $1,536,089.64.

The investigation began in May 2019, when Le took a leave of absence while facing increased scrutiny from UCSF's Audit and Advisory Services Unit, given the school's inability to reconcile tuition revenues with enrollment in the programs Le administered. The government's filings describe how, while Le was on leave, a program student provided Le's replacement a tuition check written out to Le-- the student explained that the payment was per Le's instructions. Thereafter, investigators conducted interviews of dozens of program students and completed a forensic examination of Le's bank accounts. This and additional other investigation revealed the extent of Le's fraud, and corresponding harm to the UCSF School of Nursing community. (Source)

School Superintendent & IT Director Plead Guilty To Embezzling $1 Million / Used Funds For Home Remolding, Luxury Cars, Etc. - February 1, 2024

From 2018 to 2022, Jeffery Menge served as the Assistant Superintendent and Chief Business Officer of Patterson Joint Unified School District.

In approximately 2020, Menge hired Eric Drabert to serve as IT Director for the school district.

Menge and Drabert conducted schemes to embezzle money from the school district. They used CenCal Tech LLC, a Nevada company that Menge controlled, to carry out the scheme. Menge was limited in his ability to conduct interested party transactions with the school district, so he created a fictitious person, "Frank Barnes," to serve as an executive for CenCal Tech. Menge and Drabert then used CenCal Tech to conduct more than $1.2 million in fraudulent transactions with the school district. The transactions involved double billing, over billing, and billing for items not delivered by CenCal Tech to the school district.

Menge and Drabert stole in additional ways as well. For example, they purchased high-end graphics cards and used those cards, together with other school district property and electricity, to operate a cryptocurrency "mining" farm at the school district. They then transferred the mined cryptocurrency to wallets under their own personal control. Menge also misused vehicles owned by the school district, including buying a Chevy truck at below-market value and selling it for a profit, and using a Ford Transit van as his own personal vehicle.

In total, Menge embezzled between $1 million and $1.5 million and Drabert stole between $250,000 and $300,000 during the scheme. Menge used stolen funds to remodel his home, to purchase luxury cars, including a Ferrari sports car, and for other personal uses. Drabert used stolen funds to remodel his vacation cabin, among other uses. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

Former Labor Union President Pleads Guilty To Stealing $6,500 In Union Funds To Pay Car Loan & Other Purchases - February 1, 2024

Brock Willson admitted that from about March 2020, and continuing through at least October 2021, he served in various capacities as a labor union's president, business manager / financial secretary, and coordinator of its joint apprenticeship training committee. By virtue of his high-level positions within the union, Willson had access to its bank accounts.

Willson abused his position of trust at the union to cause the local bank to make payments for his own person expenses, including but not limited to payments on his personal vehicle loan and purchases at department stores. Willson admitted stealing at least $6,500 in union funds. (Source)

BANKING / FINANCIAL INSTITUTIONS

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)

Bank Employee Sentenced To 5 Years Of Supervised Release For Embezzling $118,000+ - February 4, 2024

From approximately November 2019 to July 2022, Jacqueline Brandt used her access as a Foundation One Bank employee, to embezzle funds from customers' accounts and to steal cash from the bank. Brandt fraudulently obtained a total of approximately $118,337.52, of which Foundation One Bank was able to recover $54,235. Brandt will be required to pay at least $1,000 per month toward restitution during her sixty-month term of supervised release. (Source)

Bank Employee Sentenced To Prison For Stealing $68,000+ From Customer - February 13, 2024
Between March 2016 and July 2017, Benjamin Lara was employed as a personal banker at a bank in West Bradenton, Florida.

Through this position, Lara assisted an 85-year-old bank customer. Lara later used information gained through his position to send 31 automatic bill payment checks in his name, to his home address, from that customer's accounts. Lara also electronically transferred funds from the victim's account onto three pre-paid cards. In total, between December 2017 and July 2019, Lara stole $68,086 from the victim's bank account. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

20 Year Employee Charged With Stealing $800,000+ Worth Of Intellectual Property From Cosmetics Company To Start Her Own Company - February 21, 2024
Catalina Morales is charged with stealing more than $800,000 worth of intellectual property from her former job to allegedly build her own company.

Morales stole trade secrets, cosmetic formulas, raw materials, finished products, labels and packaging materials from the cosmetics company LaDove in Miami Lakes, Florida, which sells skincare and other products.

Morales worked for the company for 20 years, investigators said. In 2019, officials said she devised a plan to steal the company's formulas and some of their products to start her own company.
Morales quit her job in 2023 and started her own company months later. Investigators said Morales ran her new business out of a warehouse in Hialeah, Florida.

On multiple occasions, LaDove products and raw materials were seen being brought into Morales' warehouses, investigators said.

According to the police report, Morales's husband was also part of the alleged scheme.

Morales faces a long list of charges, including grand theft and embezzlement or theft of trade secrets. (Source)

Contractor For Aeronautics Company Sentenced To Prison For Roles In Conspiracy To Steal Aircraft Design / Testing - February 12, 2023
Juan Martinez was a contractor who worked as a technical lead for a small aeronautics company. With Josepth Pascua and the other conspirators, he launched a scheme to steal proprietary trade secret information from a large aircraft company for use in developing and marketing their own technology, with the intent to market and sell that technology to the true owner's competitors.

Two other conspirators are serving federal prison terms after pleading guilty in the case. Craig German and Gilbert Basaldua, 63 are serving time in prison after pleading guilty to Conspiracy to Steal Trade Secrets and Interstate Transportation of Stolen Property. (Source)

U.S. Department Of Health & Human Services Orders Medical Center To Pay $4.75 Million Because Employee Stole Protected Health Information - February 6, 2024

The U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR), announced a settlement with Montefiore Medical Center, a non-profit hospital system based in New York City for several potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

The $4.75 million monetary settlement and corrective action resolves multiple potential failures by Montefiore Medical Center relating to data security failures by Montefiore that led to an employee stealing and selling patients' protected health information over a six-month period.

In May 2015, the New York Police Department informed Montefiore Medical Center that there was evidence of theft of a specific patient's medical information. The incident prompted Montefiore Medical Center to conduct an internal investigation. It discovered that two years prior, one of their employees stole the electronic protected health information of 12,517 patients and sold the information to an identity theft ring. Montefiore Medical Center filed a breach report with OCR.

OCR's investigation revealed multiple potential violations of the HIPAA Security Rule, including failures by Montefiore Medical Center to analyze and identify potential risks and vulnerabilities to protected health information, to monitor and safeguard its health information systems' activity, and to implement policies and procedures that record and examine activity in information systems containing or using protected health information. Without these safeguards in place, Montefiore Medical Center was unable to prevent the data breach or even detect the attack had happened until years later. (Source)

Verizon Employee Gained Un-Authorized Access To 63,000+ Employees Sensitive Information / Breach Not Discovered For 3 Months - February 6, 2024

A data breach notification shared with the Office of the Maine Attorney General reveals that a Verizon employee gained unauthorized access to a file containing sensitive employee information on September 21, 2023.

Verizon discovered the breach on December 12, 2023, nearly three months later, and determined it contained sensitive information of 63,206 employees.

Verizon says it is actively working towards strengthening its internal security to prevent similar incidents from occurring again in the future and noted that at this time, there are no signs of malicious exploitation or evidence of the data having been widely leaked. (Source)

CHINESE ESPIONAGE / THEFT OF TRADE SECRETS INVLOVING U.S. GOVERNMENT / COMPANIES / UNIVERSITIES

U.S. Engineer Charged With Stealing Missile Tracking Technology Trade Secrets And Contacting China - February 7, 2024

Chenguang Gong is charged in a criminal complaint with theft of trade secrets.

Gong transferred more than 3,600 files from the research and development company where he worked to personal storage devices during his brief tenure with the company last year. The files Gong allegedly transferred include blueprints for sophisticated infrared sensors designed for use in space-based systems to detect nuclear missile launches and track ballistic and hypersonic missiles, and blueprints for sensors designed to enable U.S. military aircraft to detect incoming heat-seeking missiles and take countermeasures, including by jamming the missiles' infrared tracking ability.

As alleged in the affidavit, the victim company hired Gong in January 2023 to work at one its laboratories as an application-specific integrated circuit design manager responsible for the design, development and verification of its infrared sensors. Beginning on approximately March 30, 2023, and continuing until his termination on April 26, 2023, Gong transferred thousands of files from his work laptop to three personal storage devices, including hundreds of files after he had accepted a job on April 5, 2023, at one of the victim company's main competitors.

During the investigation, the affidavit states, the FBI discovered that, between approximately 2014 and 2022 while employed at several major technology companies in the United States, Gong submitted numerous applications to China Talent Programs' administered by the People's Republic of China government.

In 2014, while employed at a U.S. information technology company headquartered in Dallas, Texas, the affidavit states that Gong sent a business proposal to a contact at the 38th Research Institute of the China Electronics Technology Group Corporation, a high-tech research institute in China focused on both military and civilian products. (Source)

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

Veterans Affairs Medical Center Pharmacy Employee Sentenced To Prison For Role In Stealing / Selling Diabetic Test Strips Worth $427,000+ - February 7, 2024

Jennifer Robertson was employed at the Battle Creek Veterans Affairs (VA) Medical Center Pharmacy in Michigan. She was responsible for ordering supplies for veterans in need of medical care.

Beginning in June 2017, Robertson stole diabetic test strips from pharmacy inventory and arranged to meet Michelle McAllister and sell them for cash. McAllister in turn sold and shipped them to Steven Anderson in Pennsylvania. Their scheme unraveled when Robertson was caught stealing in November 2019.

In June 2023, a jury found Anderson guilty of all twelve charges against him. In total, Anderson trafficked over 7,900 boxes of stolen diabetic test strips worth over $427,795. Anderson's co-conspirators, Robertson and McAllister pled guilty and were sentenced to prison last year. (Source)

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

Employee Of Stock Trading Company Convicted Of Engaging In Unauthorized Trading That Caused $30 Million+ In Losses - February 8, 2024

Keith Wakefield worked as the head of fixed income trading for IFS Securities, Inc., a broker-dealer in Chicago.

In 2019, Wakefield knowingly and fraudulently engaged in unauthorized speculative trading in U.S. Treasury bonds using his employer's trading accounts, causing more than $30 million in losses to the employer and its counterparties. Wakefield attempted to conceal the unauthorized trades and losses by entering fake off-setting trades into a clearing broker's order system, creating the false impression that he had profitably traded through a different clearing broker. (Source)

Employee Of Oil & Gas Trading Firm Convicted For Role In Foreign $1 Million Bribery And Money Laundering Scheme - February 24, 2024

A federal jury convicted an oil and gas trader for his role in a scheme to bribe Ecuadorean and Mexican government officials and to launder money to secure contracts worth hundreds of millions of dollars for his then-employer, Vitol Inc. (Vitol), the U.S. affiliate of the largest independent energy trading firm in the world.

Javier Aguilar paid more than $1 million in bribes to officials of Petroecuador, the Ecuadorean state-owned oil and gas company, and PEMEX Procurement International (PPI), a subsidiary of PEMEX, the Mexican state-owned oil and gas company, to obtain lucrative contracts for Vitol.

Between 2015 and 2020, Aguilar was a trader in Vitol's Houston office. As a part of the scheme, Aguilar and his co-conspirators agreed to bribe senior Ecuadorian officials to obtain a $300 million contract to purchase fuel oil for Vitol. Aguilar and his co-conspirators used another Middle Eastern state-owned entity to circumvent Petroecuador's restrictions on contracts with private companies. In return for the promise and payments of bribes, the Ecuadorian officials then ensured that the Middle Eastern state-owned entity and Vitol were awarded the contract. Following the 2017 Ecuadorean presidential election, the officials who received bribes were replaced by new senior officials. To ensure continuity under the then-existing fuel oil contract and to obtain additional business, Aguilar and his co-conspirators agreed to bribe them as well.

To conceal the scheme, Aguilar and his co-conspirators used a series of fake contracts, sham invoices, and shell entities incorporated in Curacao, Panama, and Cayman Islands. Aguilar also used alias email accounts to communicate with his co-conspirators rather than his Vitol email.

The evidence at trial also demonstrated that Aguilar used the same system of shell entities and sham invoices to launder bribe payments to two officials at PPI. In total, Aguilar paid approximately $600,000 in bribes to these officials to obtain numerous contracts for Vitol to supply hundreds of millions of dollars of ethane gas to PEMEX. (Source)

Former Employee Of Youth & Family Services Organization Sentenced To Prison For $483.000+ Fraudulent Medicaid Billing Practices - January 31, 2024

Eric King, a former employee of Eye For Change Youth and Family Services, Inc., a non-profit corporation in Cleveland, was previously found guilty after a jury trial of 13 counts of health care fraud, one count of false statement relating to health care matters, and five counts of aggravated identity theft.

From June 2018 through May 2021, King defrauded Medicaid by causing Medicaid to be billed for services not actually performed or for services that were not actually performed for the amount of time the billing codes reflected; for falsifying progress notes into Medicaid beneficiary electronic records; for creating false progress notes; and for using the identities of clients without authorization to bill Medicaid. As a result of King's conduct, Medicaid paid over $483,000 for fraudulent billings. (Source)

Office Manager Sentenced To Prison For Embezzling $200,000+ Over 6 Years - February 6, 2024

Heather Migliore admitted that, between 2015 and 2021, while she was the Office Manager of a tax preparation business, that she wrote over 600 fraudulent checks for her own benefit from the business's checking accounts without her employer's knowledge or permission. Migliore also used one of the business's credit cards to make over 200 fraudulent charges. The owner of the business had to use a home equity line of credit to pay its bills during this timeframe. (Source)

Ex-Director Of Technical Education Program, Contractor & Company Plead Guilty To Theft $200,000+ From The Puerto Rico Department of Education - February 14, 2024

Kelvin Pagán-La Luz, Javier Santiago-Rodríguez, and Star Enterprises Inc. Star Enterprises) pleaded guilty to Federal Program Theft in violation of Title 18, United States Code, Section 666(a)(1).(A).

From June 2019 and continuing through August 2021, the defendants aiding and abetting each other, stole, embezzled, and obtained by fraud $213,201.07 owned by, and under the care, custody, and control of the Puerto Rico Department of Education (PRDOE).

Kevin Pagán-La Luz was employed by the PRDOE as the director of the Technical Education Program, a component of the PRDOE that was responsible for the administration of public post-secondary institutions operated under the auspices of the PRDOE. Pagán-La Luz lived with defendant Javier Santiago-Rodríguez, the owner and president of defendant Star Enterprises, a corporation with a registered physical address identical to the residential address that Pagán-La Luz and Santiago-Rodríguez shared.

In November 2017, Star Enterprises failed to renew its certificate of eligibility to contract with the PRDOE or other local governmental entities.

In December 2019, the Puerto Rico Department of State cancelled Star Enterprises certificate of incorporation because of its failure to comply with the Puerto Rico General Corporations Law.

As of December 2019, Star Enterprises could neither lawfully enter into any contracts with the government of Puerto Rico, nor lawfully conduct business in Puerto Rico. Despite not having either a valid certificate of eligibility or a valid certificate of incorporation, Kelvin Pagán-La Luz authorized payments to Star Enterprises totaling $213,210.07 for work that Star Enterprises purportedly performed for the PRDOE. In September 2020, Pagán-La Luz used an intermediary business that was an authorized contractor to funnel $59,999 to Star Enterprises and Santiago-Rodríguez for services that were never rendered. (Source)

EMPLOYEES' WHO EMBEZZLE / STEAL MONEY FOR PERSONAL ENRICHMET AND TO LIVE ENHANCED LIFESTYLE OR TO SUPPORT GAMBLING OR DEBIT PROBLEMS

Financial Fund Manager With Equity Firm Arrested In $29 Million Fraud & Gambling Probe - February 14, 2024

Sarunas Stepukonis, a Lithuanian national and former Fund Manager and partner with European private equity firm BaltCap, has been arrested and is suspected of misappropriating and gambling away $29 Million.

Estonia based BaltCap is the largest private equity firm in the Baltic region. It fired Stepukonis in November after a routine review exposed financial mismanagement. It later contacted the police when it discovered funds had been misappropriated.

In late January, companies owned by BaltCap sued Stepukonis and two casino operators, OB Holdings 1, which owns the Olybet online casino brand, and Casino Olympic Group Baltija, which has numerous land based casinos in the Baltics.

The lawsuit alleges Stepukonis deposited $17.94 million into accounts he held with the two operators, both of which still hold undefined shares of the money. It seeks to recover the missing millions, plus 6% interest.

Simonas Gustainis, managing partner at BaltCap, said he believes the casinos failed in their legal requirements to guard against money laundering and "pathological gambling tendencies."

But speaking to The Baltic Times last week, Rolandas Kiskis, head of Lithuania's financial crimes agency, said his office hadn't received a single suspicious transaction report from Olympic Casino Group, which was unusual. (Source)

Jury Convicts Corporate Chief Financial Officer And Wife Of $2.4 Million Wire Fraud Fake Invoce Scheme / Used Funds Gambling & Buying Bitcoin - February 16, 2024

Michael Tew and Kimberly Tew were found guilty for their roles in a wire fraud scheme that defrauded National Air Cargo, a logistics company and contractor for the Department of Defense.

Beginning in 2018, Michael Tew and Kimberly Tew conspired to defraud National Air Cargo through the submission of dozens of false invoices for services and items that were never provided. Over the course of two years, with the help of a co-conspirator, the Tews defrauded the business of five million dollars. The Tews gambled away much of the money and spent $2.4 million buying Bitcoin at Bitcoin ATMs across the Denver area. (Source)

Employee Charged For Embezzling $1 Million+ From Employer For 7 Years / Used Funds For Designer Clothing, Spa Services, Luxury Hotels - January 31, 2024

Monica Svobodny worked as the Supply Chain and Engineering Manager at Sico, Inc, a furniture and home furnishing manufacturing company located in Edina, Minnesota. Svobodny used her position to embezzle funds and convert them to her own use and benefit.

Svobodny regularly used company credit cards for unauthorized personal expenses such as designer clothing, spa services, and luxury hotel stays.

To cover her fraud, she left unapproved credit card expenses as "pending" for accounting purposes.

On more than 300 occasions, she used company cards to transfer funds to herself via PayPal to cover personal expenses. Svobodny also edited PayPal transaction receipts and fraudulently listed some of the expenses as payments to a defunct company.

In total, Svobodny knowingly and willfully embezzled more than $1,137,000 from Sico, Inc. over a period of seven years. (Source)

Bookkeeper Charged With Stealing $1 Million+ To Pay For Personal Expenses - February 13, 2024

From May 2020 to May 2023, Amanda Robertson used her position as a Bookkeeper to unlawfully obtain funds and services totaling over $1,000,000 from her employer's account. By accessing the company's bank accounts, she scheduled unauthorized electronic payments and issued company checks to pay her personal expenses. (Source)

Former Bookkeeper Sentenced To Prison For Embezzling $650,000+ / Used Funds For Jewelry, Etc. - February 14, 2024

Emilee Rueda was the Office Manager and in-house Bookkeeper at a small business.

Between September 2018 and February 2020, she made more than $650,000 in unauthorized expenditures on antique jewelry, lifelike dolls, trinkets, and other miscellaneous items, intending to resell many of these purchases. Rueda made false entries into the business's books to hide the theft, which was only uncovered after an employee's paycheck bounced. (Source)

Former Office Manager For County Development Foundation Pleads Guilty To Using Credit Card To Make $142,000+ Of Un-Authorized Charges For Personal Expenses - February 14, 2024

From November 5, 2012, through May 15, 2019, while employed as the Secretary / Office Manager for the Somerset Pulaski County Development Foundation (SPCDF) in Kentucky, Lisa Gadberry devised a scheme to defraud the organization by means of materially false and fraudulent representations and promises.

Gadberry utilized the SPCDF credit card for numerous unauthorized personal expenses, including personal vacations, retail purchases, gasoline, electricity, cell phone, restaurants, and entertainment expenses, and concealed her scheme by paying the bill out of an account the Pulaski Fiscal Court, the SPCDF Board, and the CPA for SPCDF did not regularly control or monitor. In total, Gadberry charged $142,874.69 in personal charges to the card. (Source)

Chik-fil-A Fast Food Manager Charged With Embezzling $140,000+ From Employer / Used Funds For Jewelry, Sports Betting, Etc. - February 4, 2024

Timothy Hill was employed by The Grove, Inc., to manage a Chik-fil-A franchise restaurant at the Minneapolis airport. As Manager, Hill was responsible for collecting and making daily cash deposits into a safe deposit box.

Between September 2022 and October 2023, Hill collected the daily cash receipts from The Grove's airport restaurants and instead of depositing it into the safe deposit box, pocketed some or all of the cash. Hill used future cash receipts to cover his theft, creating a false impression that the cash deposits were delayed rather than stolen.

Hill spent the stolen cash on jewelry, online sports betting, and the adult website Only Fans. He also transferred thousands of dollars through CashApp to various individuals, including several female colleagues in exchange for personal photos and videos.

In total, Hill knowingly and willfully embezzled approximately $144,000 from The Grove over a period of 13 months. (Source)

Employee Handling Billing & Payroll Sentenced To Prison For Inflating Hours Worked In The Amount Of $75,000 - February 13, 2024

Chelsea Sunn was employed by Blakeman's Towing and Recovery, a vehicle towing and roadside assistance business in Vermont.

Sunn was hired as a full-time office worker but later converted to part-time employment. Sunn was compensated on an hourly basis that included time and a half pay for claimed overtime work. Among other duties, Sunn handled Blakeman's billing and payroll.

Beginning no later than December 2018 and continuing at least until March 2020, Sunn defrauded Blakeman's Towing and Recovery by falsely inflating the hours she reportedly worked. This caused Blakeman's to pay Sunn tens of thousands of dollars beyond her authorized compensation.

Sunn used the interstate wire communication system to report her fraudulently-inflated work hours, and caused Blakeman's to make electronic direct deposits of fraudulently-obtained funds into Sunn's bank account in Vermont. Sunn was ordered to pay restitution in the amount of $75,000. (Source)

Employee Uses Company Credit Card To Purchase $31,000+ Of Lottery Tickets - February 7, 2024

Warren Johnson was a truck driver for All Phase Paving.

The owner of the company discovered one of the company's credit cards had several thousand dollars worth of fraudulent charges on it back in September 2023.

The owner of the company told police only three people, Johnson included, had credit cards connected to the All Phase Paving bank account. He added that the cards were intended to only be used for work-related charges. Each card had a different number, so the charges could be traced back to the employee who possessed the particular card.

The owner went through the credit card statements and noticed Johnson's card was used to charge $31,693 between several convenience stores.

The owner also reviewed the tracking information for the company vehicle Johnson drove and determined it correlated with the credit card charges.

The owner confronted Johnson about the credit card charges, he admitted to using the card to purchase lottery tickets. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

No Incidents To Report

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

Former Employee Arrested For Breaking Into Former Employer And Draining Thousands Of Gallons of Wine At Winery Costing $600,000 - February 21, 2024

The mystery man who broke into the Woodinville Winery and emptied thousands of gallons of wine in November 2023 was a former employee, according to the King County Sheriff's Office (KCSO).

Woodinville police arrested a Seattle man in his 60s Wednesday for the crime on Nov. 22, 2023 when he broke into Sparkman Cellars winery and opened valves on large containers of sauvignon blanc, which spilled and ruined the wine. According to the KCSO. Officials said the amount of lost product equaled about 24,000 bottles of wine worth $600,000.

According to the KCSO, the man was processed at King County jail and released. Charges of second-degree burglary were forwarded to King County prosecutors, the KCSO said. (Source)

THEFT OF ORGANIZATIONS ASSESTS

Former FedEx Driver Sentenced To Prison For Selling Firearms He Stole From Packages On His Truck - February 6, 2024

Frank O'Toole previously worked as a FedEx delivery truck driver at a facility in Middleborough, Massachusetts.

Between October 2021 and June 2022, O'Toole stole three packages sent from out-of-state which he was responsible for delivering, each containing a firearm – specifically, two rifles and a shotgun – intended for a Federal Firearms Licensee. O'Toole subsequently sold the three firearms to an undercover agent during two separate controlled purchases on Aug. 9, 2022 and Aug. 12, 2022. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

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)

EMPLOYEE DRUG RELATED INCIDENTS

2 Hotel Managers Sentenced To Prison For Selling Drugs From Hotel - February 14, 2024

In 2023, law enforcement agents received information that Robert Galloway and Cassie McKenzie, who were managers at a Economy Inn in Mississippi, were selling drugs from the hotel. Further investigation revealed they were selling a methamphetamine / fentanyl mixture. On June 8, 2023, agents conducted a search and found 14 grams of a methamphetamine / fentanyl mixture in two separate bags, as well as a firearm, digital scales, and additional unused distribution baggies. (Source)

OTHER FORMS OF INSIDER THREATS

No Incidents To Report

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES' NON-MALICIOUS ACTIONS CAUSING DAMAGE TO ORGANIZATION

Finance Worker Pays Out $25 Million To Fraudsters Posing As The Company's Chief Financial Officer Using Deepfake Technology - February 4, 2024

A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's Chief Financial Officer in a video conference call, according to Hong Kong police.

The elaborate scam saw the worker duped into attending a video call with what he thought were several other members of staff, but all of whom were in fact deepfake recreations, Hong Kong police said at a briefing.

(In the) multi-person video conference, it turns out that everyone [he saw] was fake, senior superintendent Baron Chan Shun-ching told the city's public broadcaster RTHK.

Chan said the worker had grown suspicious after he received a message that was purportedly from the company's UK-based Chief Financial Officer. Initially, the worker suspected it was a phishing email, as it talked of the need for a secret transaction to be carried out.

However, the worker put aside his early doubts after the video call because other people in attendance had looked and sounded just like colleagues he recognized, Chan said. (Source)

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

No Incidents To Report

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'

Former Employee At Skilled Nursing Facility Sentenced To Prison For Criminal Abuse Of A Vulnerable Adult - February 1, 2024

Kevib Thomas was employed as a Customer Service Representative and Smoking Aide at Capital City Skilled Nursing Facility (CCSNF), a residential rehabilitation and healthcare center, located in Southeast Washington. Thomas' job duties included taking individuals outside of the facility to their designated smoking area.

On November 29, 2021, a resident of the facility reported that a staff member pushed him from his wheelchair while he was attempting to enter CCSNF's smoking area. The victim has physical and psychological disabilities that would classify him as a "vulnerable adult" under D.C. Code § 22-932. During a subsequent interview, the victim stated that the staff member, identified as Thomas, pushed him and he fell out of his wheelchair and onto the ground, where he laid for several minutes without assistance from the defendant. After reviewing video of the incident, Thomas was immediately suspended from CCSNF, who then reported the abuse to the District's Department of Health. (Source)

EMPLOYEES' INVOLVED IN TERRORISM

No Incidents To Report

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

DEFINITIONS OF INSIDER THREATS

The definition of Insider Threats can be vast, and must go beyond current definitions (By Sources Such As: National Insider Threat Policy, NISPOM Conforming Change 2 & Other Sources) and be expanded.

While other organizations have definitions of Insider Threats, they can also be limited in their scope.

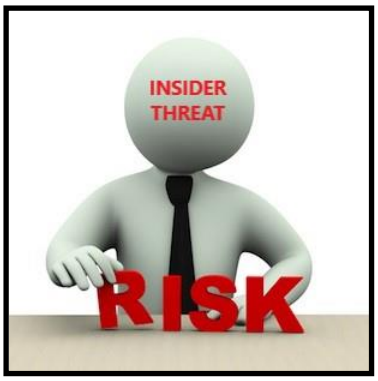
TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

- ☐ Non-Malicious But Damaging Insiders (Un-Trained, Careless, Negligent, Opportunist, Job Jumpers, Etc.)
- ☐ Disgruntled Employees' Transforming To Insider Threats
- ☐ Damage Or Theft Of Organizations Assets (Physical, Etc.)
- ☐ Theft / Disclosure Of Classified Information (Espionage), Trade Secrets, Intellectual Property, Research / Sensitive - Confidential Information
- ☐ Stealing Personal Identifiable Information For The Purposes Of Bank / Credit Card Fraud
- ☐ Financial / Bank / Wire / Credit Card Fraud, Embezzlement, Theft Of Money, Money Laundering, Overtime Fraud, Contracting Fraud, Creating Fake Shell Companies To Bill Employer With Fake Invoices
- ☐ Employees' Involved In Bribery, Kickbacks, Blackmail, Extortion
- ☐ Data, Computer & Network Sabotage / Misuse
- ☐ Employees' Working Remotely Holding 2 Jobs In Violation Of Company Policy
- ☐ Employees' Involved In Viewing / Distribution Of Child Pornography And Sexual Exploitation
- ☐ Employee Collusion With Other Employees', Employee Collusion With External Accomplices / Foreign Nations, Cyber Criminal - Insider Threat Collusion
- ☐ Trusted Business Partner Corruption / Fraud
- ☐ Workplace Violence(WPV) (Bullying, Sexual Harassment Transforms To WPV, Murder)
- ☐ Divided Loyalty Or Allegiance To U.S. / Terrorism
- ☐ Geopolitical Risks (Employee Loyalty To Company Vs. Country Because Of U.S. - Foreign Nation Conflicts)

ORGANIZATIONS IMPACTED

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

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



INSIDER THREAT DAMAGES / IMPACTS

The Damages From An Insider Threat Incident Can Many:

Financial Loss

- ☐ Intellectual Property Theft (IP) / Trade Secrets Theft = Loss Of Revenue
- ☐ Embezzlement / Fraud (Loss Of $$$)
- ☐ Stock Price Reduction

Operational Impact / Ability Of The Business To Execute Its Mission

- ☐ IT / Network Sabotage, Data Destruction (Downtime
- ☐ Loss Of Productivity
- ☐ Remediation Costs
- ☐ Increased Overhead

Reputation Impact

- ☐ Public Relations Expenditures
- ☐ Customer Relationship Loss
- ☐ Devaluation Of Trade Names
- ☐ Loss As A Leader In The Marketplace

Workplace Culture - Impact On Employees'

- ☐ Increased Distrust
- ☐ Erosion Of Morale
- ☐ Additional Turnover
- ☐ Workplace Violence (Deaths) / Negatively Impacts The Morale Of Employees'

Legal & Liability Impacts (External Costs)

- ☐ Compliance Fines
- ☐ Breach Notification Costs
- ☐ Increased Insurance Costs
- ☐ Attorney Fees
- ☐ Employees' Loose Jobs / Company Goes Out Of Business

DISSATISFACTION, REVENGE, ANGER, GRIEVANCES (EMOTION BASED)

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

MONEY / GREED / FINANCIAL HARDSHIPS / STRESS / OPPORTUNIST

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

IDEOLOGY

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

COERCION / MANIPULATION BY OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

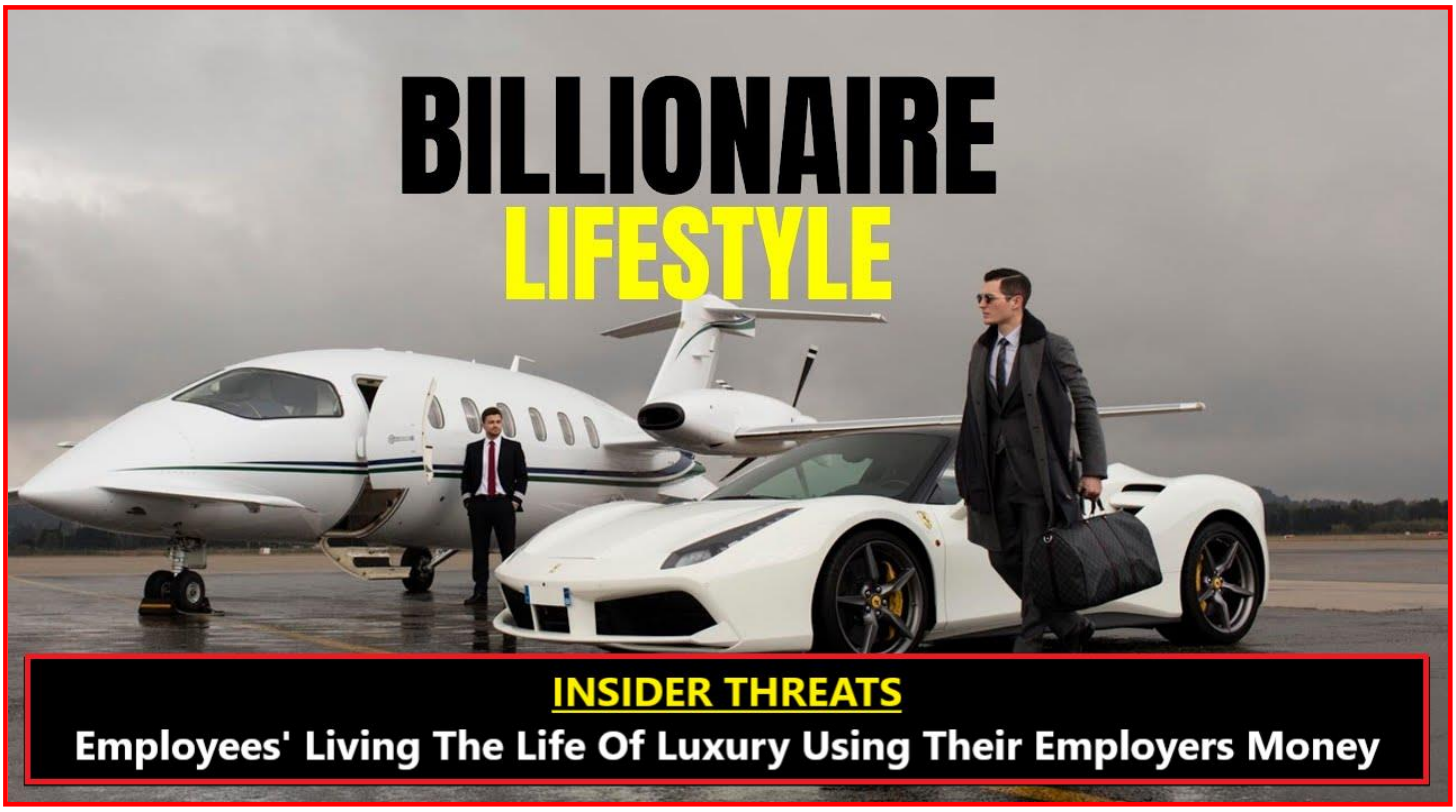
- ☐ Bribery, Extortion, Blackmail

COLLUSION WITH OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

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

OTHER

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



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

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

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

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

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

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

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEE EXTORTION

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

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

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

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

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

Several days after the FBI executed the search warrant at Sharps's residence, Sharp caused false news stories to be published about the incident and his company's response to the Incident and related disclosures. In those stories, Sharp identified himself as an anonymous whistleblower within company, who had worked on remediating the Incident. Sharp falsely claimed that his company had been hacked by an unidentified perpetrator who maliciously acquired root administrator access to his company's AWS accounts. Sharp in fact had taken the his company's data using credentials to which he had access in his role as his company AWS Cloud Administrator. Sharp used the data in a failed attempt to his company for $2 Million. (Source)

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

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

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

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

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

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

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

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

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

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

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

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

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

Former Credit Union Employee Pleads Guilty To Unauthorized Access To Computer System After Termination & Sabotage Of 20+GB's Of Data/ Causing $10,000 In Damages (2021)

Juliana Barile was fired from her position as a part-time employee with a New York Credit Union on May 19, 2021.

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

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

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

Fired IT System Administrator Sabotages Railway Network - February 14, 2018

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

UNDERAPPRECIATED / OVERWORKED / NO OVERSIGHT

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

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

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

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

DESTRUCTION OF EMPLOYERS PROPERTY BY EMPLOYEES

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

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

Investigation revealed that several files had been purposefully stacked on the boardroom table, all of which were burned in the fire. The bank was scheduled for a review by the Texas Department of Banking the very next day. The investigation revealed that Moody had created false nominee loans in the names of several people, including actual bank customers. Moody eventually admitted to setting the fire in the boardroom to conceal her criminal activity concerning the false loans.

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

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

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

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

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

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)

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)

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

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

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

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

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

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

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

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

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

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

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

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

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

In reality, SFCU had not met all conditions precedent to closing and had suffered a material adverse effect. Unbeknownst to the United States Department of the Treasury, the SFCU was in a financial crisis. From 2015 through 2017, another individual who was the Chief Financial Officer (CFO) of SFCU had been falsifying reports. In addition, she was creating fictitious entries in the banks records to support the false reports.

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

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

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

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

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

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

Former Controller Of Oil & Gas Company Sentenced To Prison For $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)

WORKPLACE VIOLENCE

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)

Doctor Working At Surgical Facility Arrested For Injecting Poison Into IV Bags Of 11 Patients / Resulting In 1 Death / Was In Retaliation For Medical Misconduct Probe - September 27, 2022

Raynaldo Rivera Ortiz Jr., is a Texas Anesthesiologist. He was arrested on criminal charges related to allegedly injecting nerve blocking and bronchodilation drugs into patient IV bags at a local surgical center, resulting in at least one death and multiple cardiac emergencies.

On or around June 21, 2022 a 55 year old female coworker of Ortiz, experienced a medical emergency and died immediately after treating herself for dehydration using an IV bag of saline taken from the surgical center. An autopsy report revealed that she died from a lethal dose of bupivacaine, a nerve blocking agent.

Two months later, on or around Aug. 24, 2022 an 18 year old male patient experienced a cardiac emergency during a scheduled surgery. The teen was intubated and transferred to a local ICU. Chemical analysis of the fluid from a saline bag used during his surgery revealed the presence of epinephrine, bupicavaine, and lidocaine.

Surgical center personnel concluded that the incidents listed above suggested a pattern of intentional adulteration of IV bags used at the surgical center. They identified about 10 additional unexpected cardiac emergencies that occurred during otherwise unremarkable surgeries between May and August 2022 .

The complaint alleges that none of the cardiac incidents occurred during Dr. Ortiz's surgeries, and that they began just two days after Dr. Oritz was notified of a disciplinary inquiry stemming from an incident during which he allegedly "deviated from the standard of care" during an anesthesia procedure when a patient experienced a medical emergency. The complaint alleges that all of the incidents occurred around the time Dr. Ortiz performed services at the facility, and no incidents occurred while Dr. Ortiz was on vacation.

The complaint further alleges that Dr. Ortiz had a history of disciplinary actions against him, and he had expressed his concern to other physicians over disciplinary action at the facility, and complained the center was trying to "crucify" him.

A nurse who worked on one of Dr. Ortiz's surgeries told law enforcement that Dr. Ortiz refused to use an IV bag she retrieved from the warmer, physically waving the bag off. A surveillance video from the center's operating room hallway showed Dr. Ortiz placing IV bags into the stainless-steel bag warmer shortly before other doctors' patients experienced cardiac emergencies.

The complaint alleges that in one instance captured in the surveillance video, Dr. Ortiz was observed walking quickly from an operating room to the bag warmer, placing a single IV bag inside, visually scanning the empty hallway, and quickly walking away. Just over an hour later, according to the complaint, a 56-year-old woman suffered a cardiac emergency during a scheduled cosmetic surgery after a bag from the warmer was used during her procedure. The complaint alleges that in another instance, agents observed Dr. Ortiz exit his operating room carrying an IV bag concealed in what appeared to be a paper folder, swap the bag with another bag from the warmer, and walk away. Roughly half an hour later, a 54-year-old woman suffered a cardiac emergency during a scheduled cosmetic surgery after a bag from the warmer was used during her procedure. (Source)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FBI Indianapolis Special Agent in Charge Paul Keenan said Hole's focus on proving his masculinity was partially connected to a failed attempt to live on his own, which ended with him moving back into his old house. Investigators also learned Hole aspired to join the military. Authorities said he had been eating MREs, or meals ready-to-eat, like those consumed by members of the armed forces.

Keenan also said Hole had suicidal thoughts that "occurred almost daily" in the months leading up to the shooting. The police had previously responded to Hole's home in March 2020 on a mental health check. Hole was put under an immediate detention at a local hospital and a gun he had recently bought was confiscated. Hole would later buy more guns and use them in the FedEx shooting, according to police. (Source)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

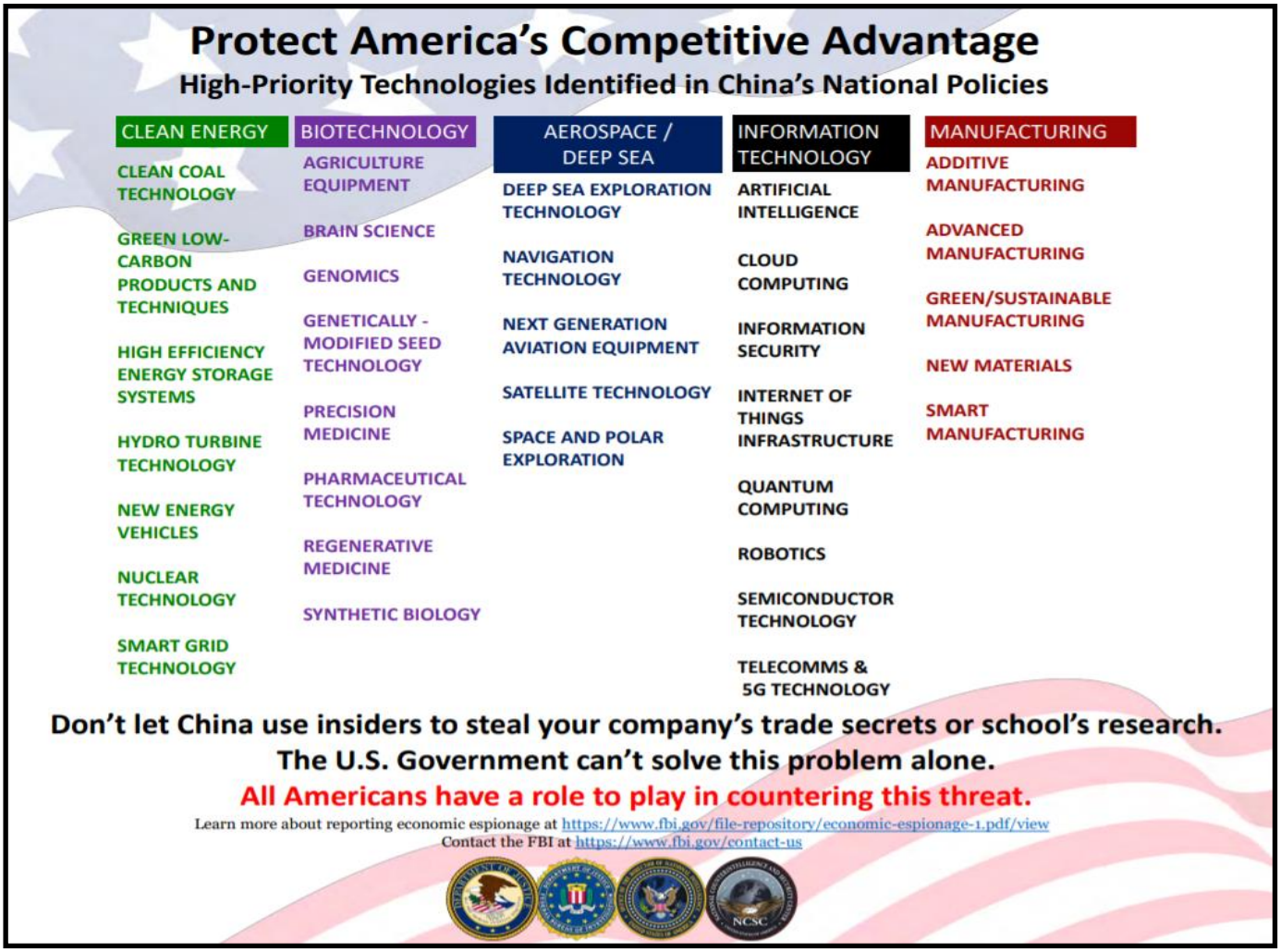
WORKPLACE VIOLENCE TODAY E-MAGAZINE
https://www.workplaceviolence911.com/node/994

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

CTTP = China Thousand Talents Plan

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

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



SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

The websites listed below are updated monthly with the latest incidents.

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present / Updated Daily

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**5,000+ Incidents**).

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

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

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

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

INSIDER THREAT INCIDENTS SPOTLIGHT REPORT FOR 2023

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

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

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

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

Incident Posting Notifications

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

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

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

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER

Updated Daily

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

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

https://www.nationalinsiderthreatsig.org/crticial-infrastructure-insider-threats.html

National Insider Threat Special Interest Group (NITSIG)

NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center. The mission of the NITSIG is to provide organizations and individuals with a ***central source*** for Insider Risk Management (IRM) guidance and collaboration.

The NITSIG Membership (**Free**) is the largest network (**1000+**) of IRM professionals in the U.S. and globally. We our proud to be a conduit for the collaboration and sharing of IRM information, so that our members can contribute to building a common body of knowledge for IRM. 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 Threat Program (ITP) Development, Management & Optimization
- ✓ ITP Working Group / Hub Operations
- ✓ Insider Risk / Threat Assessments & Mitigation Strategies
- ✓ Insider Threat Detection Tools (UAM, UBA, DLP, SEIM) (Requirements Analysis & Purchasing Guidance)
- ✓ Insider Threat Awareness and Training
- ✓ Workplace Violence Guidance / Active Shooter Response Guidance & Training

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

The NITSIG has created a LinkedIn Group for individuals that interested in sharing and gaining in-depth knowledge regarding IRM and Insider Threat Program Management (ITPM). This group will also enable the NITSIG to share the latest news, upcoming events and information for IRM and ITPM. We invite you to join the group. https://www.linkedin.com/groups/12277699

The NITSIG is the creator of the "***Original***" Insider Threat Symposium & Expo (ITS&E). The ITS&E is recognized as the ***Go To Event*** for in-depth real world guidance from ITP Managers and others with extensive ***Hands On Experience*** in IRM.

At the expo are many great vendors that showcase their training, services and products. The link below provides all the vendors that exhibited at the 2019 ITS&E, and provides a description of their solutions for Insider Threat detection and mitigation.
https://nationalinsiderthreatsig.org/nitsiginsiderthreatvendors.html

The NITSIG had to suspend meetings and the ITS&E from 2020 to 2023 due to ongoing COVID outbreaks. We are working on resuming meetings in the later part of 2024, and looking at holding the ITS&E in 2024.

NITSIG Insider Threat Mitigation Resources
Posted on the NITSIG website are various documents, resources and training that will assist organizations with ITP Development, Management, Optimization and IRM.
http://www.nationalinsiderthreatsig.org/nitsig-insiderthreatsymposiumexporesources.html

Employee Risk / Threat Mitigations Is Our Business

The Insider Threat Defense (ITDG) Group is considered a ***Trusted Source*** for Insider Risk Mitigation (IRM) training and consulting services.

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

White House, U.S. Government Agencies, Department Of Homeland Security, TSA, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines,) Intelligence Community (DIA, NSA, NGA) Universities, FBI, U.S. Secret Service, DEA, Law Enforcement, Critical Infrastructure Providers, Universities, Fortune 100 / 500 companies and others; Microsoft Corporation, Walmart, Home Depot, Nike, Tesla Automotive Company, Dell Technologies, Nationwide Insurance, Discovery Channel, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more. The ITDG has provided training and consulting services to over **650+** organizations. (Client Listing)

Over **900+** individuals have attended our highly sought after Insider Threat Program (ITP) Development, Management & Optimization Training Course (Classroom & Live Web Based) and received ITP Manager Certificates. (Training Brochure)

With over **14+** years of experience providing IRM training and consulting services, we approach the Insider Threat problem and IRM from a realistic, operational and holistic perspective. A primary centerpiece of providing our clients with a comprehensive IRM Framework, is that we incorporate lessons learned based on our analysis of ITP's and Insider Threat related incidents encountered from working with our clients.

Our IRM training and consulting services have been recognized, endorsed and validated by the U.S. Government and businesses, as some of the most ***affordable, comprehensive and resourceful*** available. These are not the words of the ITDG, but of our clients. ***Our client satisfaction levels are in the exceptional range***. We encourage you to read the feedback from our students on this link.

ITDG IRM Training / Consulting Services Offered

Training / Consulting Services (Conducted Via Live Instructor Led Classroom / Onsite / Web Based)

- ✓ IRM Training Workshops For CEO's, C-Suite & ITP Managers / Working Group, Insider Threat Analysts & Investigators
- ✓ ITP Development, Management & Optimization Training Course & Related Training Courses
- ✓ IRM Framework Training (For Organizations Not Interested In Developing An ITP)
- ✓ Insider Risk - Threat Vulnerability Assessments That Go Beyond Compliance Regulations For IRM
- ✓ ITP Gap Analysis Assessments
- ✓ Malicious Insider Playbook Of Tactics Assessment / Mitigation Guidance
- ✓ Insider Threat Awareness Training For Employees'
- ✓ Insider Threat Detection Tool Guidance / Pre-Purchasing Evaluation Assistance
- ✓ Customized IRM Consulting Services For Our Clients

Additional Background Information On ITDG

Mr. Henderson is the Founder and Chairman of National Insider Threat Special Interest Group (NITSIG), and Founder / Director of the Insider Threat Symposium & Expo (ITS&E). The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center.

The NITSIG Membership is the largest network (**1000+**) of IRM Professionals in the U.S. and globally. Combining NITSG Meetings, ITS&E Events and ITDG Training Courses / Consulting Services, the NITSIG and ITDG have provided IRM Guidance and Training to **3,300+** individuals.

In 2024, Mr. Henderson created the U.S. Insider Risk Management Center of Excellence (USIRMCOE). The USIRMCOE Advisory Board is comprised of some of the leading Insider Risk Management (IRM) Professionals in the private sector, who are currently managing or supporting IRM Programs.

One of the core mission goals of the USRIMCOE is to collaborate and build strategic partnerships with IRM Professionals, allowing the USIRMCOE to serve as a Trusted Partner / Information Sharing and Analysis Center for IRM.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Threat Program (ITP) Development, Management & Optimization Training Course Instructor
Insider Risk / Threat Vulnerability Assessment Specialist
ITP Gap Analysis / Evaluation & Optimization Specialist
LinkedIn ITDG Company Profile
Follow Us On Twitter / X: @InsiderThreatDG

Founder / Chairman Of The National Insider Threat Special Interest Group
Founder / Director Of Insider Threat Symposium & Expo
Founder U.S. Insider Risk Management Center Of Excellence
Insider Threat Researcher / Speaker
LinkedIn NITSIG Group

Contact Information
561-809-6800
www.insiderthreatdefensegroup.com
jimhenderson@insiderthreatdefensegroup.com
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org