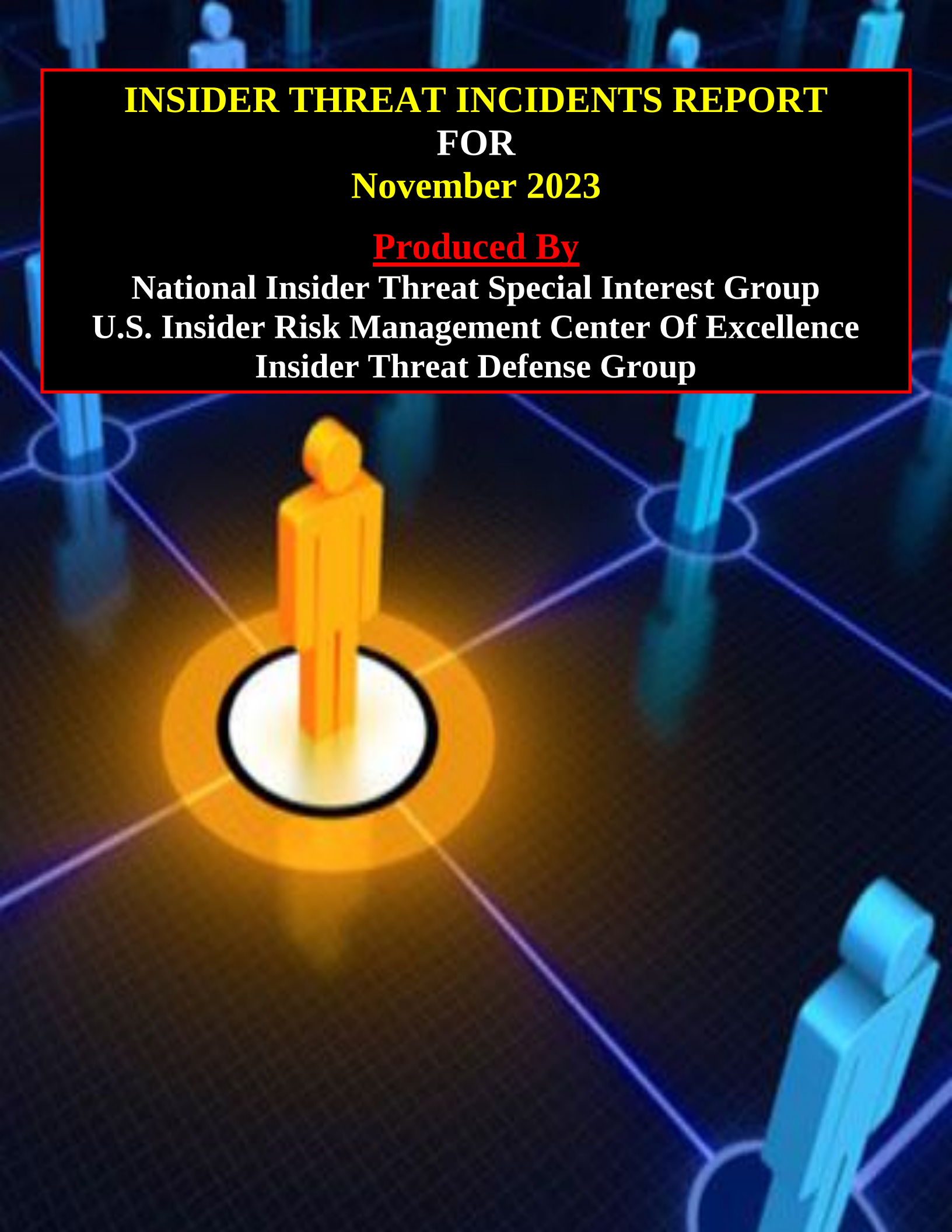
INSIDER THREAT INCIDENTS REPORT
FOR
November 2023

Produced By

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



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 10+ years. This research has evaluated and analyzed over **4,900+** 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 incident listed on pages **7 to 24** 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.

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.

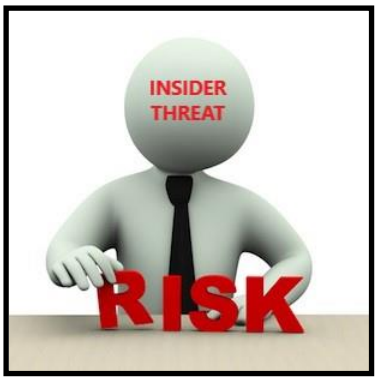
TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

- ☐ 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

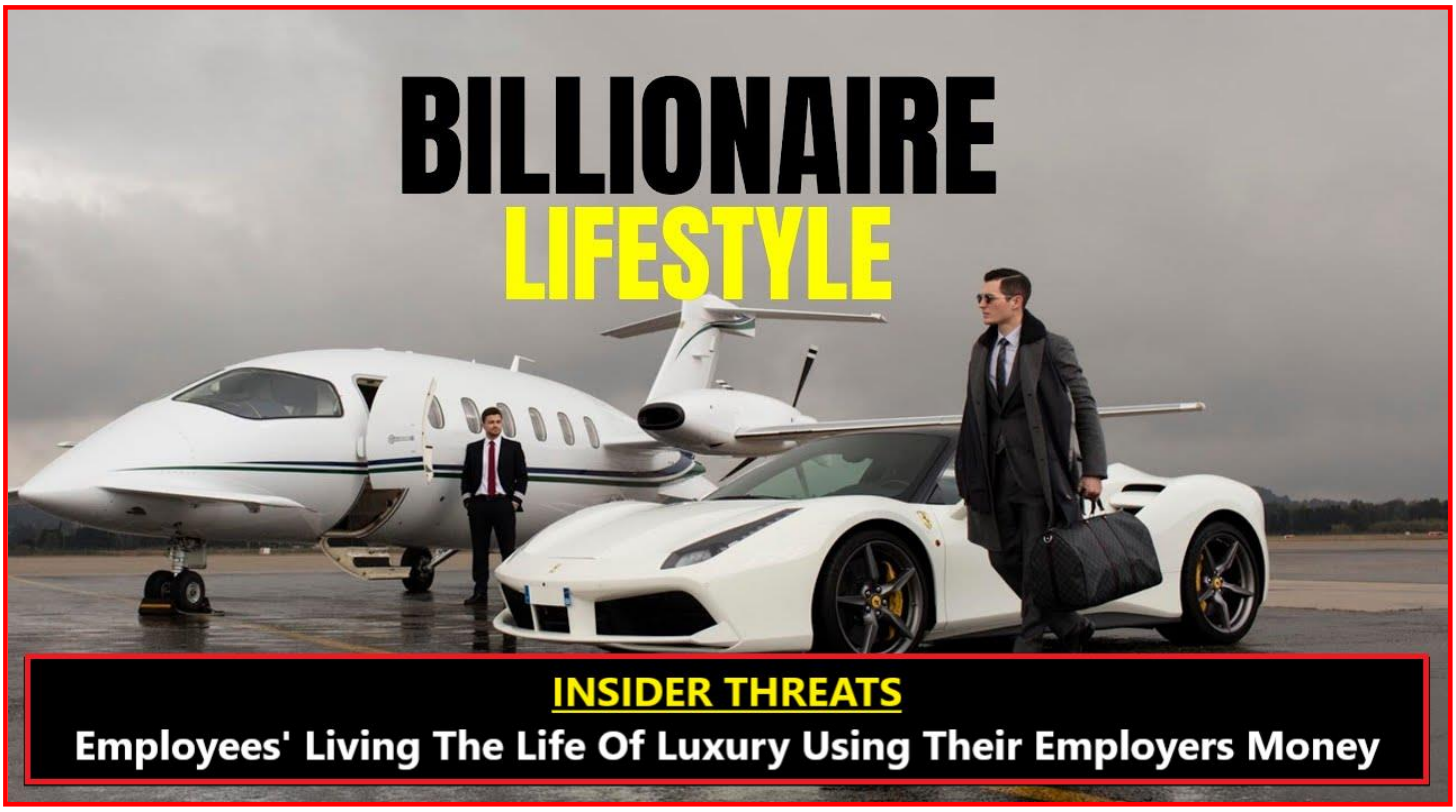
- ☐ Public Relations Expenditures
- ☐ Customer Relationship Loss
- ☐ Devaluation Of Trade Names
- ☐ Loss As A Leader In The Marketplace

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



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

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

INSIDER THREAT INCIDENTS
FOR NOVEMBER 2023

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

Royal Canadian Mounted Police Official Found Guilty Releasing Classified Information - November 22, 2023

A jury has found former RCMP intelligence official Cameron Jay Ortis guilty of breaching Canada's secrets law.

Jurors declared Ortis guilty of three counts of violating the Security of Information Act and one count of attempting to do so. They also found him guilty of breach of trust and fraudulent use of a computer.

Ortis had pleaded not guilty to all charges, including violating the secrets law by revealing classified information to three individuals in 2015 and trying to do so in a fourth instance.

He testified he offered secret material to targets in a bid to get them to use an online encryption service set up by an allied intelligence agency to spy on adversaries. But Ortis lacked authority to disclose classified material and that he was not doing so as part of a sanctioned undercover operation. (Source)

Australia Government Report Stated That Disgruntled Employees In Critical Infrastructure Are Being Targeted By Foreign Spies On Dark Web - November 1, 2023

The Australia Government has released its first review into the dangers faced by Australia's critical infrastructure, such as the nation's hospitals, its energy and telecommunications organisations and its food delivery networks.

Australia's national intelligence agency says espionage has supplanted terrorism as its principle national security concern, and that even a small level of activity could have severe consequences that may take years to be resolved.

The review found dark web job advertisements listed by foreign intelligence services are targeting "disgruntled employees" as a recruitment tool, seeking to take advantage of either a desire for money or revenge.

It also found the growing trend of working from home had led to more connection between work and personal devices, making insider threats more difficult to detect.

Over the last two years, chat forum platforms like Discord and War Thunder have seen classified or sensitive information leaked, often by people with legitimate access to the information they leaked. The reviewers said the intention of people leaking in chat forums differed, but was sometimes driven by a need to show off, or prove a point in an argument. (Source)

U.S. GOVERNMENT

U.S. Postal Employee And 2 Co-Conspirators Arrested For $24 Million+ Stolen Check Scheme - November 17, 2023

From March 2021 to July 2023, Nakedra Shannon was employed by the U.S. Postal Service (USPS) as a mail processing clerk at a USPS processing and distribution center in Charlotte, NC.

From April to July 2023, Shannon conspired with Donnell Gardner and Desiray Carter to steal incoming and outgoing checks from the U.S. mail, which Gardner and Carter then sold to other individuals including using the Telegram channel OG Glass House.

Over the course of the conspiracy, the co-conspirators allegedly stole checks totaling more than $24 million, including more than $12 million in stolen checks which were posted for sale on the Telegram channel OG Glass House, and more than $8 million in stolen U.S. Treasury checks. The indictment also alleges that the defendants obtained hundreds of thousands of dollars in criminal proceeds of the mail theft scheme. (Source)

U.S. Postal Employee Convicted For Conspiracy, Bank Fraud, Aggravated Identity Theft & Theft Of Postal Service Key - November 17, 2023

Kristen Williams was employed as a mail carrier at the post office in Alabama

In late October 2022, Williams stole and sold a USPS arrow key to a coconspirator. Arrow keys are government property and will open all blue USPS collection boxes in a particular geographic area. Williams's coconspirator, who previously pleaded guilty to bank fraud conspiracy and aggravated identity theft, paid Williams $2,500 in cash for the key. Law enforcement caught Williams's coconspirator using the key to steal mail from collection boxes outside a mall in November 2022. The coconspirator stole hundreds of pieces of mail using the key.

Williams also conspired to commit bank fraud involving counterfeit checks deposited into her bank account. The counterfeit checks were derived from checks stolen from the mail. (Source)

U.S. Postal Service Employee Convicted Of Embezzling $90,000+ Of Money Orders - November 1, 2023

Jamesa Rankins began working for USPS around 2016, most recently as a Sales & Service Distribution Associate. In this role, Rankins had the ability to generate postal money orders, including replacement money orders.

Customers could obtain replacement money orders without paying any additional fees if the original money orders were lost, damaged or erroneous. Rankins issued over $90,000 worth of replacement money orders to another individual where the original money orders were not erroneous and had not been lost or stolen. On at least one occasion, Rankins personally negotiated one of the replacement money orders at a check cashing business.

Rankins also applied for and obtained unemployment assistance from the Massachusetts Division of Unemployment Assistance, despite being employed by USPS and thus being ineligible to receive unemployment assistance.

Rankins embezzled over $90,000 and fraudulently obtaining unemployment benefits. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

U.S. Army Maintenance Worker Pleads Guilty To Using Fuel Credit Card To Make $33,000+ Of Un-Authorized Fuel Purchases - November 14, 2023

Normas Dais was employed by the United States Army as a civilian maintenance worker at the Fort Lesley J. McNair Department of Public Works.

Dais repeatedly purchased gasoline for private vehicles using a General Services Administration fuel credit card meant solely for a designated maintenance van on the Fort McNair grounds. Investigators found that from April to October of 2023, Dais frequently arranged to meet private vehicles at area gas stations and used his General Services Administration credit card to purchase their gas. In total, Dais made more than 400 unauthorized purchases totaling at least $33,868.21. As part of the plea agreement, Dais agreed to pay full restitution. (Source)

CRITICAL INFRASTRUCTURE

Pilot Who Tried To Crash Plane With 83 People On Board Had Taken Magic Mushrooms 2 Days Earlier / Had Depression Problems - November 11, 2023

The off-duty Alaska Airlines pilot who is accused of trying to shut down a plane's engine last month has given his side of the story, telling The New York Times that he thought he was only imagining the journey and needed to take drastic action to bring the dream to an end.

Joseph Emerson was riding in the jump seat of Horizon Air Flight 2059, an Alaska Airlines affiliate, when he allegedly tried to pull two handles that would have engaged a fire-suppression system and cut fuel to the engines.

Tragedy was averted when the pilots apprehended Emerson and landed the aircraft safely in Portland, Oregon. Emerson has since pleaded not guilty to 83 counts of attempted murder, 83 counts of reckless endangerment and one count of endangering an aircraft in relation to the incident.

"I thought it would stop both engines, the plane would start to head towards a crash, and I would wake up," Emerson told The New York Times during an interview at the county jail in Portland, where he is being held without bail.

Emerson said he was desperate to awaken from a hallucinogenic state that had consumed him since taking psychedelic mushrooms, known as magic mushrooms two days earlier.

Emerson stated that after his friends death, he dealt with a therapist who suggested he go to a doctor to be diagnosed with depression. He considered it, but a diagnosis may have stopped him from flying due to F.A.A. rules. He said he instead self-treated his grief and mental health issues with alcohol, although he said he does not consider himself an alcoholic and never let it affect his ability to fly. (Source)

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Former Sheriff's Employee Sentenced To Prison For Theft Of $150,000+ In Official Funds - November 17, 2023

While employed at the West Baton Rouge Parish Sheriff's Office, Nicole Miller stole cash ($158,852) paid for traffic tickets and hid the thefts by recording fraudulent journal entries in the Sheriff's Office accounting system. Miller's scheme began on or about July 1, 2018, and continued through in or about September 2022. (Source)

Former Corrections Officer Sentenced To Prison For Smuggling Contraband Into Prison / Received $10,000 in Bribe Payments - November 21, 2023

Krystle Burrell was a Corrections Offices at the Anna M. Kross Center on Rikers Island.

Burrell accepted nearly $10,000 in bribes from co-conspirators on behalf of co-defendant Terrae Hinds in exchange for Burrell smuggling contraband into the prison for Hinds. Burrell also accepted payments on behalf of Hinds for narcotics and other contraband so that Hinds could resell the contraband on Rikers Island. After she pleaded guilty in federal court in September 2022 to bribery charges and while on bail pending sentencing, Burrell conspired with Hinds and others to smuggle contraband into the federal Metropolitan Detention Center in Brooklyn where Hinds had been transferred and was being held on federal charges. In March 2023, Burrell was charged with the additional crime of smuggling contraband into a federal prison. (Source)

Prison Correctional Officer Sentenced To Prison For Accepting $9,800 In Bribes From Inmates To Smuggle Tobacco

In late 2021, Shauna Boatright was assigned to monitor an inmate in the facility's Residential Drug Abuse Program.

Boatright told the inmate that she was in financial distress and asked him how she could make some money. Boatright agreed to take bribes to smuggle tobacco into the prison for the inmate. Inmates are prohibited from possessing tobacco in federal prisons. Boatright later took bribes to smuggle tobacco into the prison for a second inmate. After the inmates received the contraband, they directed their associates outside of the facility to transfer money to Boatright using CashApp. Between September 30 and October 27, 2021, Boatright received five CashApp payments from the inmates' associates totaling $9,800. (Source)

Police Officer / Union President Charged With $5,000+ Of Overtime Fraud - November 28, 2023

Paul Helring while serving as the coordinator of Scranton Police Department's extra duty overtime program, knowingly obtained by fraud over $5,000.00 in compensation paid to him for extra duty patrol shifts at several local, lower-income housing complexes that Helring claimed to work but did not in fact work. (Source)

STATE / CITY GOVERNMENTS / MAYORS

Former State Employee Sentenced To Prison For Role In $800,000+ Unemployment Insurance Fraud Scheme For Personal Use - November 9, 2023

New York State Department of Labor (NYSDOL) employee Wendell Giles was sentenced today to 36 months in prison for engaging in a fraudulent scheme to obtain more than $800,000 in unemployment insurance benefits by abusing his position with the NYSDOL.

Giles admitted that he and another former NYSDOL employee, Carl DiVeglia abused their state computer systems access to create and approve false unemployment insurance applications in 2020 and 2021, including applications for the federal Pandemic Unemployment Assistance (PUA) program.

Giles recruited relatives, friends and friends-of-friends to submit false benefits applications over the phone to DiVeglia, after Giles had instructed them to lie in response to eligibility questions. Giles and DiVeglia then took a share of the benefits paid by NYSDOL on the false claims.

Giles used his share to enrich himself, including by purchasing a three-wheeled motorcycle. (Source)

Former City Commissioner Sentenced To Prison For Role $480,000+ Contracting Bribery Conspiracy - November 30, 2023

Gerardo Tafolla along with former Weslaco City commissioner John Cuellar, accepted bribes from Arturo Cuellar, Ricardo Quintanilla and others in exchange for official action favorable to engineering companies seeking large contracts with the city.

From approximately March 2008 through December 2015, one of the participants in the scheme received approximately $4.1 million from two engineering companies and shared nearly $1.4 million with Arturo Cuellar, a former Hidalgo County commissioner. Arturo Cuellar then used a company he controlled to facilitate the payment of approximately $405,000 in bribes to his cousin, John Cuellar, which were disguised as legitimate legal expenses. In exchange for these payments, John Cuellar took several official actions to benefit the companies, including helping to award contracts worth approximately $38.5 million to rehabilitate Weslaco's water treatment facilities.

Quintanilla received approximately $85,000 during the course of the scheme and used that money to pay cash bribes to Tafolla for his official actions to benefit the companies that received the water treatment plant contracts. (Source)

City Public Health Investigators / Inspectors Admit To Receiving $50,000+ Of Illegal Overtime Payments - November 28, 2023

Michael Ingram, a Public Health Investigator for Trenton's Bureau of Environmental Health (BEH), and William Kreiss, a registered environmental specialist for BEH, conducted residential lead inspections with other members of BEH from February 2018 through May 2022.

The BEH employee to whom Ingram and Kreiss reported began directing them to bill overtime hours for work they did not perform. Ingram and Kreiss submitted their fraudulent and inflated overtime claims to this BEH employee, who then authorized overtime payments to each of them.

Ingram and Kreiss each admitted submitting claims for overtime work as directed by the BEH employee, including for work they had not performed. Ingram and Kreiss also admitted they had inflated claims for overtime hours worked in connection with a meal delivery program administered by the city.

Through this fraudulent overtime scheme, Ingram admitted he received $22,144 in overtime payments to which he was not entitled, while Kreiss separately admitted he received $32,806 in overtime payments to which he was not entitled. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

Former University Employee Sentenced To Prison For Embezzling $326,000+ In Donations For 4 Years For Herself - November 9, 2023

Teresa Maners was employed with the Indiana University Foundation as a Depositor and Payroll Deduction Associate beginning in 1988.

The Indiana University Foundation works to maximize financial support for Indiana University through private donations and on-campus fundraisers. Maners' job duties included recording cash and checks received from donors and preparing them for deposit in the foundation's bank account.

During her employment, Maners stole hundreds of thousands of dollars from the foundation by taking cash before recording it in the foundation's accounting systems.

To hide the stolen cash, Maners secretly withheld checks from the day's deposits and substitute those checks in a subsequent day's deposit to hide the missing cash. She also wrote checks to the foundation from her personal bank account to cover any difference between the substituted donor checks and the stolen cash. This type of fraud is sometimes referred to as a "lapping scheme." As the only employee in charge of recording cash donations, Maners was able to alter the accounting paperwork to "balance" the books and keep the stolen cash donations for herself. Maners continued the fraud for nearly four years, and stole approximately $326,334 from the foundation. In 2019, the foundation conducted an external audit after discovering accounting irregularities, and confronted Maners who admitted to stealing the money. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

Labor Union Official Pleads Guilty To Embezzling $3,000+ - November 2, 2023

October 29, 2021, Jason Weaver used his position as Secretary / Treasurer of Local Union 1509 of the American Postal Workers Union to write out a check for $352.62 to himself from cal 1509 bank account. Weaver signed his name as an authorized account signatory and forged the name of another union officer who was also an authorized account signatory.

Weaver admitted that he knew he was not entitled to the money, and that he deposited the check into his personal bank account. Weaver further admitted to writing 12 other checks totaling $2,679.32 from 1509's bank account to himself and forging the names of other authorized account signatories between April 25, 2016, and May 19, 2021. (Source)

BANKING / FINANCIAL INSTITUTIONS

Former Bank Manager Pleads Guilty To Facilitating $12.4 Million Covid Fraud Scheme / Unemployment Benefits Fraud Scheme - November 8, 2023

Anthony Brockman is former bank Branch Manager. He pleaded guilty to accepting Kansas City Chiefs playoffs tickets and a new Chevrolet Tahoe in exchange for facilitating a $12.4 million Covid fraud scheme by a business owner, as well as a separate fraud scheme to receive unemployment benefits.

Brockman also admitted that he fraudulently received $11,040 in unemployment benefits from March 27, 2020, to Nov. 4, 2021, while he was employed by US Bank. Brockman falsely claimed he was unemployed when he applied for unemployment benefits via the internet, then repeated that false claim in 11 subsequent weekly online applications submitted to the state. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

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

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

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

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

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

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

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

Nippon Telegraph & Telephone Employee Downloaded & Leaked Company Data For 10 Years Because Of Security Failures - November 20, 20233

A prolonged, systemic failure in data security management resulted in a 10-year leak of personal information in about 9 million cases stored at a subsidiary of Nippon Telegraph and Telephone West Corp. (NTT West).

The security breach occurred at NTT Business Solutions in Osaka, which handles maintenance and operation of the computer system for call centers.

A former temporary employee working at the firm had illegally taken out private information, such as addresses, names and telephone numbers, from the computer system where the data for the call centers was stored.

It is believed that the information was sold to list brokers, a type of business or individual involved in the trade or sales of personal information and data lists. Police are looking into the case.

According to the NTT side's explanation, the former temporary employee downloaded the lists onto a work terminal and then transferred the data to a personal USB memory device.

NTT did not implement measures to prevent downloads to terminals or connections of personal USB devices, nor did it have a system to detect suspicious activities such as mass data processing. It also neglected to monitor records of access to the system.

NTT group claims it had instructed these protective measures to be taken, but they were not thoroughly implemented. (Source)

5 Employees Steal Company Data To Start Their Own Business - November 21, 2023

The sequence of events sounds like it was taken straight from a movie script. 5 software programmers were working late into the night, chatting on their phones while they worked.

During the wee hours of October 9, between 1:00 am and 4:00 am, they managed to hack the company's primary server and successfully gained access to sensitive customer data, which they then proceeded to steal.

The following day, all 5 software company employees in Chennai showed up to work in Bengaluru or Chennai, where they joined their coworkers in expressing their shock and horror at the loss of sensitive information belonging to five of the company's most valuable clients.

The business owner had no idea what was happening as he saw his six years of hard work go down the drain. His workforce mostly defected.

Then he discovered that his US-based clients had been cut off because the operating system he used, Amazon Web Services (AWS), had changed their credentials. He tried to contact them but was met with silence.

He eventually went to the police in Chennai, India, about the cybercrime. The investigators followed the internet protocol address and other technical facts from where the server was accessed and gained a breakthrough within a few hours.

Local authorities narrowed it down to five people: two in Chennai and three in Bengaluru, all firm employees. Edison who was responsible for the company's operations in Chennai, was the one who logged onto the server and began the theft. According to their findings, he participated in a conference call with four other people.

Using this information, they were able to track down his coworker in Chennai, Ramkumar, as well as three employees at the Bengaluru office: Kavya Vasanthkrishan, Ravitha Devasenapathy, and S Karuppaiah.

Police discovered that the five had formed a new software firm called "Blue Dawn" the day following the theft and had contacted the five victims, whose information had been taken, offering their services at a steep discount. (Source)

Real Estate Firm Sues Former Broker & Rival Company For Alleging Stealing Trade Secrets - November 9, 2023

An Illinois real estate firm has filed a lawsuit against a former employee for allegedly stealing trade secrets and redirecting business to its competitors.

Tammy Mitchell Hines & Co. filed the lawsuit against Logan S. Goff, Kimberly M. Benda, and Epic Realty, LLC, citing allegations of civil conspiracy, breach of contract, common law fraud, conversion, false-light invasion of privacy, tortious interference with contract, and trade secret misappropriation.

Goff was hired to work as a real estate broker for Tammy Mitchell Hines & Co. (TMH) on June 12, 2021.

The plaintiff asserts that disputes began to arise between TMH and Goff. The suit states that between June 2022 and October 2022, Goff allegedly downloaded and stole TMH's database of customers, hundreds of active leads, and other trade secrets owned by TMH and provided the information to defendants Benda and Epic Realty. During this time, Goff also allegedly contacted TMH customers and clients for the purpose of directing their business to Benda and Epic Realty and conducted other activities to damage TMH's name, brand and reputation

TMH is seeking a judgment in this case for damages in excess of $50,000, plus interest, court costs, attorney fees, and any other relief the court deems proper. (Source)

When A News Reporter Becomes An Insider Threat / Medical Center Settles Allegations It Violated HIPAA Privacy Rule - Pays $80,000 Penalty - November 20, 2023

St. Joseph's Medical Center in New York has chosen to settle allegations it violated the HIPAA Privacy Rule and has agreed to pay a $80,000 financial penalty and adopt a corrective action plan to address the aspects of non-compliance discovered by OCR during its investigation.

On April 20, 2020, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) launched an investigation following the publication of an Associated Press (AP) article about how the medical center was responding to the COVID-19 pandemic. The article, which included images, revealed information about the medical center's response but also patient information, including patients' COVID-19 diagnoses, current medical statuses and medical prognoses, vital signs, and treatment plans.

The article, which was distributed nationally, suggested St. Joseph's Medical Center had provided an AP reporter with access to three patients and their clinical information. OCR investigated to determine whether the patients concerned had provided authorization for their information to be disclosed to the reporter. OCR determined that St. Joseph's Medical Center had provided the AP reporter with access to the patients and their PHI but had not obtained a HIPAA-compliant authorization from the patients.

Since HIPAA does not permit the disclosure of protected health information to the media and the patients had not authorized the disclosures, the medical center was found to have violated the HIPAA Privacy Rule. (Source)

CHINESE ESPIONAGE TARGETING U.S. GOVERNMENT / COMPANIES / UNIVERSITIES

No Incidents To Report

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

No Incidents To Report

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

Employee Steals $3.7 Million From Employer - November 28, 2023

Tanisha Adderley worked for a health and human services technology solutions company that recovered fees paid by their clients and remitted refunds to them via wires from their funds recovery bank account. Ms. Adderley had access to the funds recovery bank account and was responsible for obtaining approvals and processing fee refunds.

Over the course of five years, from 2019 to 2023, Adderley prepared false approvals and processed wire payments to non-vendor business bank accounts that were controlled by Ms. Adderley.

Adderley fraudulently obtained $3.7 million in company funds. (Source)

Employee For Investment Firm Charged With Stealing $3 Million+ From Clients -November 16, 2023

From July 2017 through March 2021, Kenneth Welsh, while serving in his capacity as an investment advisor employed by a large brokerage firm, misappropriated at least $3 million from five clients. Welsh, who had been entrusted to manage client funds responsibly, instead perpetrated a scheme to defraud the five clients by diverting money from their brokerage accounts to accounts under his control. (Source)

Former Law Firm Office Manager Pleads Guilty To Embezzling $1.1 Million+ From Law Firm For 11 Years - November 21, 2023

Jairo Santos admitted to embezzling more than $1.1 million from his employer, a San Francisco-based law firm, where Santos worked as the Office Manager.

Santos began embezzling from his employer in March of 2016 and continued with his scheme through February 2023.

Santos obtained checks from the victim law firm, filled out the payee line of those checks, addressing them to "Jairo Santos," and signed each check with the signature of the law firm's senior partner even though Santos was not authorized to do so. Santos then deposited these checks into his personal checking accounts at Wells Fargo Bank. Santos admitted to depositing approximately 806 fraudulent and unauthorized checks from the victim law firm made payable to Santos into his personal checking accounts. The total value of these unauthorized deposits was approximately $1,191,683. Santos deposited these checks from the victim law firm knowing that the payments were not authorized by the firm or its senior partner. (Source)

Salesman For Home Builder Sentenced To Prison For $1 Million Fraud / Kickback Conspiracy - November 28, 2023

From 2018 to 2020, Edmundo De La Torre admitted he was working as a salesman for a homebuilder.

De La Torre used his position to attempt to get potential customers approved for Department of Housing and Urban Development (HUD)-backed mortgages. He forged various documents, including financial statements, bank statements, paycheck stubs and letters of reference for at least 38 otherwise unqualified homebuyers.

De La Torre then submitted these fake and forged documents to an area bank on behalf of the potential homebuyers. He admitted he was receiving a commission for each sale and personally profiting over $200,000 from the scheme. In addition, more than three dozen known loans in this scheme ultimately defaulted or had to be restructured, costing HUD roughly $971,310.10 at the time of his plea. (Source)

Goldman Sachs Investment Banker Sentenced To Prison For $280,000 Insider Trading Scheme - November 1, 2023

Brijesh Goel was an Investment Banker at Goldman Sachs in New York.

In that position, Goel received confidential internal emails directed to Goldman Sachs' Firmwide Capital Committee and Credit Markets Capital Committee. These e-mails contained detailed information and analysis about potential merger-and-acquisition transactions that Goldman Sachs was considering financing.

Goel misappropriated this confidential information and tipped a friend, Akshay Niranjan, who worked at another investment bank in New York, with the names of potential target companies.

Niranjan then used that confidential information to trade call options, including short-dated, out-of-the-money call options, in brokerage accounts that were in the name of Niranjan's brother. Goel and Niranjan agreed to split the profits from their trading. Between approximately 2017 and 2018, Goel tipped Niranjan on at least six deals in which Goldman Sachs was involved, yielding total illegal profits of approximately $280,000. (Source)

Former Utah Home Owners Association Treasurer Admits To Stealing Over $230,000 - November 2, 2023

Sharon Gordon embezzled approximately over $232,000 from four Lava Bluff Home Owners Association (HOA) bank accounts between 2016 and March 2022.

Gordon diverted the funds electronically by transferring them directly to her personal account, writing checks to herself and her boyfriend and forging other board members' signatures, depositing checks representing HOA member fees directly into her personal accounts, writing checks to casinos from HOA accounts, and withdrawing cash from HOA accounts.

Gordon is also ordered to pay the remaining $63,448.32 from the $232,078 in restitution to Lava Bluff HOA. To date, Gordon has paid the HOA $168,629.68 in restitution. (Source)

2 Former San Francisco Department of Building Inspection Construction Engineers Charged With Accepting Bribes - November 3, 2023

2 of Building Inspection (DBI) Construction Plan Engineers have been charged with accepting bribes in return for expediting and approving building and construction plan permits.

Rodolfo Pada began accepting bribes in 2003 and continued to do so until he retired in September 2017. The bribes consisted of cash, free meals, drinks, and other benefits bestowed upon Pada by executives at a construction planning and design firm in return for Pada expediting and approving permits for building and construction plans. Pada is alleged to have solicited, accepted, and concealed an interest-free $85,000 loan facilitated by a construction planning and design firm executive.

Cyril Yu began accepting bribes in January 2018 and continued to do so until February 2021.

The bribes consisted of cash, free meals, drinks, and other benefits bestowed upon Yu by executives at a construction planning and design firm in return for Yu expediting and approving permits for building and construction plans. (Source)

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

Chief Marketing Officer Pleads Guilty To Embezzling $10 Million +/ Used Funds To Buy Yacht, Mercedes-Benz & Amphibious Plane - November 28, 2023

Brinson, Silver was the Chief Marketing Officer of Root, Inc., an online car insurance company.

From November 2021 through November 2022, Silver entered into contracts with four vendors for marketing services. Silver directed the vendors to send a portion of their contract proceeds to bank accounts in the names of businesses that Silver owned and controlled. Those diverted payments totaled more than $10.2 million.

Silver used the millions he embezzled to buy a $1.4 million dollar yacht, a Mercedes-Benz G550 for nearly $165,000, an amphibious plane, luxury watches and other items.

As a result of his fraud scheme, in February 2023, Root sued Silver. The Court granted a motion in his civil suit that limited him to financial transactions no greater than $5,000. Silver failed to appear in court for a hearing related to his civil suit and instead spent lavishly while traveling the globe.

His expenditures in February and March 2023 violated the Court's orders and include $20,000 on plastic surgery, more than $25,000 at Indonesian businesses (including $8,000 at a luxury resort in Bali) and in withdrawals made in Indonesia, and more than $88,000 through PayPal to individuals. Silver also withheld from the Court information about a $1.8 million house he owned in California. During this time, Silver also made two phone calls to an "international relocation" company and asked for citizenship within a country that would not extradite him to the United States, and a foreign bank account that the United States could not freeze. (Source)

Former Office Manager Pleads Guilty To Embezzling $3.5 Million+ / Used Fund For Daughters Wedding, Travel, Bought Vehicle, Etc. - November 30, 2023

Between 2015 and 2020, while employed as an Office Manager and Executive Assistant at an Alpharetta, a Georgia company providing yard care services, Sonya Hesenius made fraudulent charges on corporate credit cards and caused the company to reimburse her personal credit card for personal expenses.

To conceal her scheme, she coded and approved all the charges herself, withheld supporting documentation from the company, and disguised the unauthorized expenditures in the company's system as legitimate expenses, such as newspaper advertisements. Hesenius also disseminated the expenditures among different job sites to further conceal the fraud.

Hesenius used the embezzled funds to pay for a variety of personal expenses, including, among other things, her daughter's wedding at the Barnsley Resort; cash transfers through PayPal, Venmo, and Square; Luis Vuitton and Chanel handbags; plane flights for Hesenius and more than 20 of her family members and friends; season tickets for University of Tennessee football and basketball teams; a recreational vehicle; hotels; furniture; cruises; and clothing items. In total, Hesenius embezzled more than $3,500,000. (Source)

Office Manager Pleads Guilty To $955,000+ Embezzlement Scheme For Personal Enrichment - October 31, 2023

Erin Sullivan was employed as the Office Manager for a family-owned construction business.

Beginning in 2016, Sullivan made false entries into the company's payroll and accounting system that caused the system to generate hundreds of fraudulent checks payable to her or to Petty Cash. Immediately after she generated a fraudulent check, Sullivan changed the reference in the payroll and accounting system to show that it had been issued to a different payee.

Sullivan sometimes generated checks in the name of the company's owner, forged the signature of company's owner on the checks, and either cashed the checks or deposited them into her bank account.

She also altered the payroll and accounting system in other ways, which resulted in her receiving additional pay to which she was not entitled. Through this scheme, Sullivan embezzled $955,960.71 from the company. (Source)

Company Accountant Pleads Guilty To Stealing $715,000+ From Medical Practice To Pay Her Credit Cards - November 21, 2023

Between May 2020 and March 2023, Carol Casilla was employed as an Accountant by Spokane Dermatology Clinic (SDC), a dermatological practice located in Spokane, Washington.

While employed at SDC, Casilla used her position to fraudulently issue company checks to herself and deposit them into her own personal accounts, and to make electronic funds transfers using company funds toward her personal credit cards.

Some of the transfers were made to a fictitious company that Casilla created in order to make it appear as though the transfers were for legitimate company expenditures. Casilla made hundreds of fraudulent transfers in this manner, stealing more than $715,000 in total. (Source)

City Manager & Employee Charged With Stealing $450,000 Of City Funds / Used Funds Vacations, Bills, Jewelry, Etc. - November 16, 2023

From 2014 to 2022, John Suplizio, the City Manager of DuBois, Pennsylvania, and Roberta Shaffer, a city employee, conspired to divert and steal hundreds of thousands of dollars in city funds.

As the full-time salaried City Manager, Suplizio maintained substantial authority in DuBois, where he ran the city's day-to-day operations.

Beginning as early as 2008, Suplizio and Shaffer used the city's tax identification number to establish secret bank accounts into which they diverted city money, including approximately $60,000 in annual administrative fees from the city's waste management contract. Suplizio and Shaffer made large cash withdrawals from these unaudited accounts, wrote checks to themselves and others, and obtained cashier's checks with themselves listed as payees totaling more than $350,000.

The defendants also allegedly spent more than $450,000 from the accounts toward payments on Suplizio's personal credit card, which he used to pay for personal vacations, utility bills for his residence, department store purchases, and jewelry store purchases, among other personal expenses. (Source)

Bookkeeper Charged For Un-Authorized Use Of Company Credit Cards / Amazon Accounts ($445,000) For Personal Enrichment - November 3, 2023

Deborah Kloor worked as a bookkeeper for a company.

Kloor used the company's credit cards as well as the owner's bank and Amazon accounts without authorization, for her own personal benefit. The indictment alleges that, from approximately January 2015 through December 2019, Kloor misappropriated $446,324.04 from the company and from the owner without their knowledge or permission. (Source)

Former Transit Authority Retirement Plan Employee Sentenced To Prison For Fraudulently Obtaining $356,000+ In Plan Funds For Herself - November 8, 2023

Ayanna Nesbitt was a clerk for the Retirement Plan for Chicago Transit Authority (CTA).

Nebitt created and obtained approval for approximately 43 fraudulent requests for the Plan to issue various benefits to CTA employees or their beneficiaries, including pension and death benefit payments, and refunds of pension contributions.

The fraudulent requests contained false representations about the purported recipients' identities and entitlement to the payments.

Nesbitt had the payments sent to financial accounts she controlled or else had the money paid to others and then transferred to Nesbitt. From 2019 to 2021, Nesbitt defrauded the Plan of approximately $356,934. (Source)

Business Manager Sentenced To Prison For Embezzling $280,000 To Buy Boat - November 16, 2023

Matthew Olinger pleaded guilty to a felony wire fraud charge and admitted embezzling from his employer in two ways. Olinger worked for a seed company as an area business manager, managing field sales representatives and occasionally purchasing agricultural equipment for the seedsmen, employees who sold seeds to regional customers.

Olinger fraudulently misused his company credit card to make at least $180,000 worth of personal purchases on hundreds of occasions, including family meals, vacations, clothing, boating expenses and personal entertainment, his plea agreement says. Olinger covered up the personal purchases by submitting fake or altered receipts to the company.

Olinger also stole company funds to help a seedman buy a 2022 Cobalt R35 boat and a trailer.

Olinger authorized an employee to sign a contract with a seedman that would have misappropriated $75,000 in company funds each year for a decade, or a total of $750,000, to buy the Cobalt boat and the trailer and pay associated boating expenses. Olinger stole $100,000 in company funds by submitting three fraudulent funding requests to his employer for a "seed tender" and "seed equipment" before his scheme was discovered by the company.
(Source)

Former Credit Union Assistant Branch Manager Pleads Guilty Tor Embezzling $60,000+ To Spend On TikTok - November 6, 2023

Andrade Olson began working at the credit union in 2005 and was promoted to Assistant Branch Manager in 2019.

Olson pleaded guilty to embezzling over $60,000 from multiple members' accounts at a credit union where she was previously employed

Olson made several unauthorized withdrawals from four members' accounts from July through August 2022.

Olson made unauthorized cash withdrawals by bringing up the victims' accounts while assisting other credit union members who were at the teller window to make it appear as though she had legitimate reasons to access the credit union's cash stores.

When confronted by credit union officials, Olson claimed that one of the victims was "doing some remodeling," but told another employee that she was "done" and abruptly resigned from her position. Olson spent most of the money that she stole on TikTok, gifting much of the funds to an out of state individual with hundreds of thousands of followers on TikTok. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Program Director Pleads Guilty To $242,000+ Wire Fraud & Money Laundering Scheme - November 21, 2023

James Matison was the Program Director for Restoration Programs at WildEarth Guardians, a not-for-profit which relies on funding from federal agencies, the State of New Mexico and other not-for-profit organizations.

As Program Director, Matison was responsible for approving all Restoration Program project invoices submitted by contractors for payment. One such contractor was Timberline Environmental, LLC, a Colorado based environmental company owned and operated by Matison's co-defendant, Jeffrey Ham.

In 2015, Matison was experiencing financial difficulties and asked Ham for help with a fraudulent scheme to obtain money from WildEarth Guardians.

Ham agreed to allow Matison to generate fraudulent invoices from Timberline for submission to and payment from WildEarth Guardians, which Matison would approve for payment. Matison would collect the checks and deposit them into Timberline's bank account. Ham provided Matison with pre-signed blank Timberline checks which Matison would use to write checks to an entity called Euro-American Development, an Arizona company under Matison's control. In this manner, Matison obtained $242,210 from WildEarth guardians between Feb. 2015 and Feb. 2019 when Ham put a stop to the scheme. (Source)

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

Former Public School Information Technology Manager Charged Sabotaging School's Computer Network - November 29, 2023

Conor LaHiff was employed as a Desktop & Network Manager at a public high school until he was terminated in June 2023.

After he was fired, LaHiff allegedly used his administrative privileges to deactivate and delete thousands of Apple IDs from the school's Apple School Manager accoun, software used to manage student, faculty and staff information technology resources. LaHiff also allegedly deactivated more than 1,400 other Apple accounts and other IT administrative accounts and disabled the school's private branch phone system, which left the school's phone service unavailable for approximately 24 hours. (Source)

THEFT OF ORGANIZATIONS ASSESTS

Former County Roads Division Employee Sentenced To Prison For $2.3 Million+ Fraud Scheme - November 8, 2023

Kevin Gunn and fellow Wayne County employee John Gibson engaged in a scheme to use taxpayer dollars to make unauthorized purchases of generators and other power equipment from retailers in southeast Michigan which they sold for hundreds of thousands in personal profit.

Between January 2019 and August 2021, Gunn solicited Wayne County vendors to purchase generators and other power equipment the vendors were not authorized to provide under their contracts with the county. To conceal the scheme to defraud, Gunn instructed the vendors to list on their invoices only the items they were authorized to sell as part of their Wayne County contracts. Roads Division employees approved and paid each vendor's invoice with taxpayer funds.

After these fraudulent purchases were verified and approved by Roads Division employees, Gibson took possession of the equipment, paid Gunn for the items, and resold the generators and other items to members of the public.

Between January 2019, and August 2021, Wayne County vendors bought 596 generators, and a variety of other power equipment including lawnmowers, chainsaws, and backpack blowers. The purchase of these items was not authorized under any vendor contract with Wayne County nor were the items ever provided to or used by Wayne County. The total value of equipment obtained as part of the scheme was over $2.3 million. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG RELATED INCIDENTS

Former Hotel Managers Plead Guilty To Conspiracy To Distribute Controlled Substances - November 1, 2023

In 2023, agents began investigating drug activity at an Economy Inn.

Agents received information that Pernell Galloway and his girlfriend, Cassie McKenzie, who were both managers at the hotel, were also selling drugs from the hotel. Law Enforcement began doing controlled purchases of a methamphetamine / fentanyl mixture from the Galloway and McKenzie.

On or about June 8, 2023, a search warrant was executed at the Economy Inn where Galloway and McKenzie were located. Agents also located an additional 14 grams of a methamphetamine/fentanyl mixture in two separate bags. Agents also located a firearm, digital scales, and additional unused distribution baggies. (Source)

Former Employee Of Money Services Business Charged With Conspiring To Launder Drug Proceeds - November 1, 2023

Yessenia Lainez is a former employee / Teller of a money services business. She worked their until May 2023.

She and used her position to launder the drug proceeds of an unnamed co-conspirator, who was a drug trafficker and who was arrested in possession of narcotics on June 1, 2023.,
Lainez wired significant sums of cash to various foreign bank accounts, including some in Mexico, at the unnamed co-conspirator's direction.

Lainez charged her co-conspirator an under-the-table fee to process the wires, each of which she structured to "evade certain reporting requirements. (Source)

Hospital Nurse Sentenced To Prison For Stealing Morphine, Fentanyl & Hydromorphone - November 15, 2023

Beginning in May 2019, Andrea Falzano used her capacity as a Nurse in the emergency department at a Massachusetts based hospital to withdraw controlled substances from a locked drug cabinet. These substances included morphine, fentanyl and hydromorphone, all of which are opioids and Schedule II controlled substances. In total, Falzano withdrew these substances 412 times for 299 already discharged patients over an approximately five-month period.

Negative drug tests uncovered during the investigation indicated that Falzano did not self-administer the drugs that she stole from the hospital at which she was employed, despite stating otherwise to her employer and the Board of Registration in Nursing. In statements to the Board, Falzano attempted to minimize her conduct by calling her theft of controlled substances an "isolated incident," which it was not. (Source)

OTHER FORMS OF INSIDER THREATS

No Incidents To Report

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS

No Incidents To Report

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

Former Account Manager Sentenced To Prison For Embezzling $3 Million+ For 10 Years / Employees Lost Jobs - November 30, 2023

Judy Green worked as an Account Manager for a Houston based building and maintenance supply company.

Green submitted fraudulent invoices to induce payment from the company and pocketed the funds for personal expenses. Ultimately, authorities uncovered the scheme when one of the business owners noticed a large payment to an unknown credit card company in the summer of 2022. An audit revealed the fraud had been ongoing since 2012.

At the hearing, the court heard additional evidence that because of the her theft, the victim company had to lay off employees and could not give bonuses to the remaining employees. (Source)

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'

No Incidents To Report

EMPLOYEES' INVOLVED IN TERRORISM

No Incidents To Report

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

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

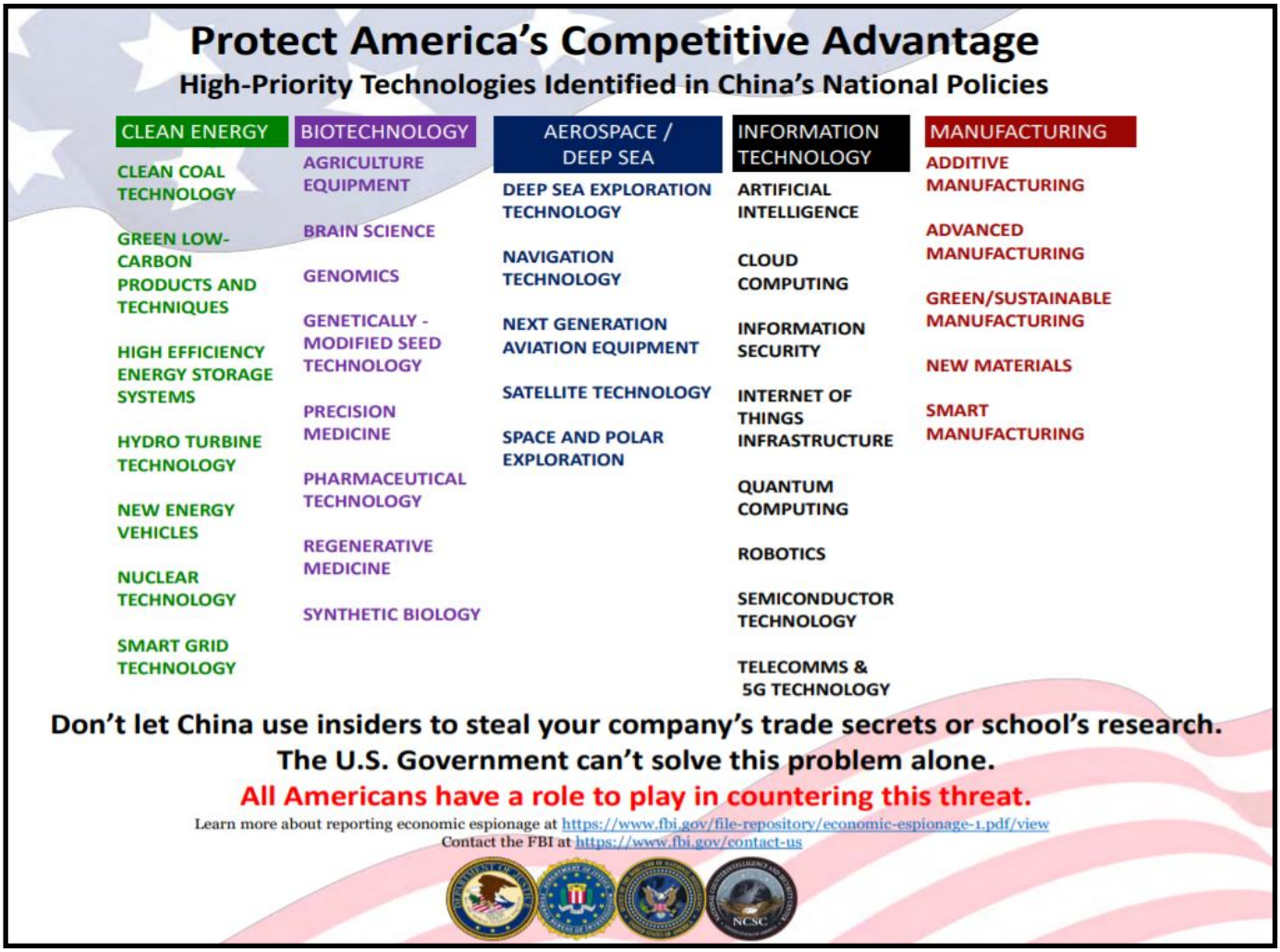
WORKPLACE VIOLENCE TODAY E-MAGAZINE
https://www.workplaceviolence911.com/node/994

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 (**4,900+ 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 Threat Mitigation (ITM) guidance and collaboration.

The NITSIG Membership (**Free**) is the largest network (**1000+**) of ITM professionals in the U.S. and globally. We our proud to be a conduit for the collaboration of ITM information, so that our members can share and gain information and contribute to building a common body of knowledge for ITM. Our member's willingness to share information has been the driving force that has made the NITSIG very successful.

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

- ✓ Insider Threat Program (ITP) Development, Implementation & Management
- ✓ ITP Working Group / Hub Operation
- ✓ Insider Threat Awareness and Training
- ✓ ITM Risk Assessments & Mitigation Strategies
- ✓ User Activity Monitoring / Behavioral Analytics Tools (Requirements Analysis, Guidance)
- ✓ Protecting Controlled Unclassified Information / Sensitive Business Information
- ✓ 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 ITM and Insider Threat Program Management (ITPM). This group will also enable the NITSIG to share the latest news, upcoming events and information for ITM 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 ITM.

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 in 2020 to 2022 due to the COVID outbreak. We are working on resuming meetings in the later part of 2023, 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 their Insider Threat Program Development / Management and Insider Threat Mitigation efforts.
http://www.nationalinsiderthreatsig.org/nitsig-insiderthreatsymposiumexporesources.html

Security Behind The Firewall Is Our Business

The Insider Threat Defense (ITDG) Group is considered a ***Trusted Source*** for Insider Threat Mitigation (ITM) training and consulting services to the: 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, Fortune 100 / 500 companies and others; Microsoft Corporation, Walmart, Home Depot, Nike, Tesla Automotive Company, Dell Technologies, 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 Training Course (Classroom Instructor Led & Live Web Based) and received ITP Manager Certificates. (Training Brochure)

With over **10+** years of experience providing training and consulting services, we approach the Insider Threat problem and ITM from a realistic and holistic perspective. A primary centerpiece of providing our clients with a comprehensive ITM 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 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 Training / Consulting Services Offered

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

- ✓ ITM Training Workshops For CEO's, C-Suite & ITP Managers / Working Group, Insider Threat Analysts & Investigators
- ✓ ITP Development - Management / ITM / Insider Threat Investigator & Related Training Courses
- ✓ ITM Framework Training (For Organizations Not Interested In Developing An ITP)
- ✓ Insider Threat Vulnerability - ITP Maturity Assessment / Mitigation Guidance
- ✓ Malicious Insider Playbook Of Tactics Assessment / Mitigation Guidance
- ✓ Insider Threat Awareness Training For Employees'
- ✓ Insider Threat Detection Tool Guidance / Pre-Purchasing Evaluation Assistance
- ✓ Customized ITM Consulting Services For Our Clients

For additional information on our training, consulting services and noteworthy accomplishments please visit this link.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Threat Program (ITP) Development / Management Training Course Instructor
Insider Threat Vulnerability - ITP Maturity Assessment / Mitigation Specialist
Insider Threat Researcher / Speaker
Founder / Chairman Of The National Insider Threat Special Interest Group (NITSIG)
NITSIG Insider Threat Symposium & Expo Director / Organizer
888-363-7241 / 561-809-6800
www.insiderthreatdefensegroup.com / jimhenderson@insiderthreatdefensegroup.com
www.nationalinsiderthreatsig.org / jimhenderson@nationalinsiderthreatsig.org