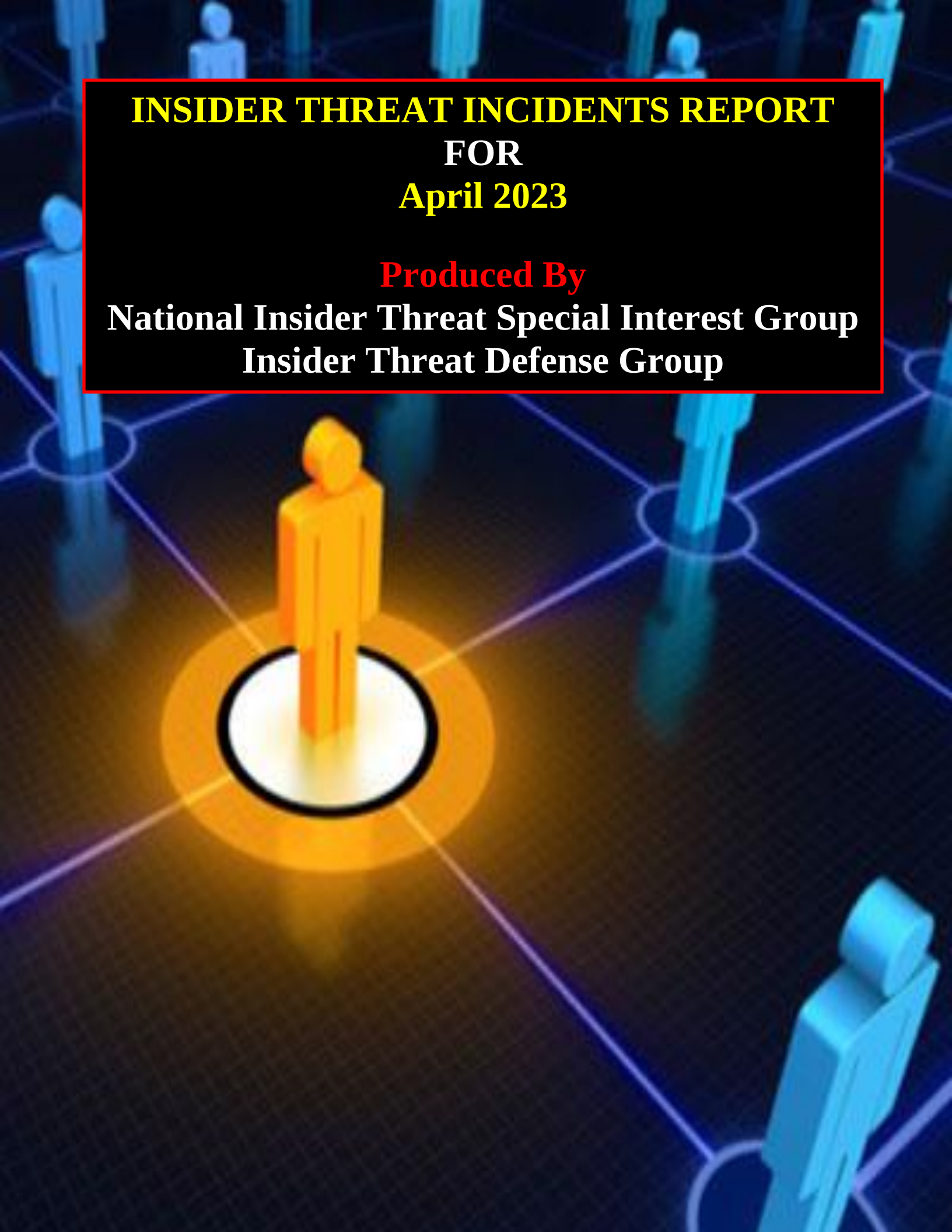


INSIDER THREAT INCIDENTS REPORT
FOR
April 2023

Produced By

National Insider Threat Special Interest Group
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 sit behind firewalls or telework through firewalls. 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 **4,500+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations and businesses of all sizes.

The NITSIG and ITDG maintain the largest public repositories of Insider Threat incidents, and receive a great deal of praise for publishing these incidents on a monthly basis to our various websites. This research provides interested individuals with a "***Real World***" view of the how extensive the Insider Threat problem is.

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 most 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.

Another problem is how surveys and reports are written on the Insider Threat problem. Some simply cite percentages of how they have increased and the associated remediation costs over the previous year. In many cases these surveys and reports only focus on the technical aspects of an Insider stealing data from an organization, and leave out many other types of Insider Threats. Surveys and reports that are limited in their scope of reporting do not give the reader a comprehensive view of the "***Actual Malicious Actions***" employees' are taking against their employers.

If you are looking to gain support from your CEO and C-Suite for detecting and mitigating Insider Threats, and want to provide them with the justification, return on investment, and funding ($$$) needed for developing, implementing and managing an ITP, the incidents listed on pages 5 to 21 of this report should help. The cost of doing nothing, may be greater then the cost of implementing a comprehensive Insider Threat Mitigation Framework.

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 CC2 & 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
- ☐ 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 / Airline Industry (Pilots, Flight Attendants)
  - 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)
- ☐ 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

INSIDER THREAT INCIDENTS
FOR APRIL 2023

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

INDIA

4 Employees' Arrested For Stealing, Sharing Manufactureing Company's Information With Competitors - April 12, 2023

According to company's complaint, the employees stole vital company information from the company's head office and shared it with competitors. The 4 employees worked for the manufacturing unit that supplies high-end technology systems and solutions to defense and security forces.

According to the complaint filed by Mukesh Sharma, he operates a manufacturing unit in New Sangvi. The employees' worked in his company and together they tarnished the company's image and created defects in the company's product that were meant to demonstrate to the client, resulting in loss for the company.

The company had fired one of the employees and to settle the score they shared the company's vital information with competitors. (Source)

U.S. GOVERNMENT

Former U.S. Postal Service Mail Carrier Sentenced To Prison For Role In Stealing $200,000+ From Her Mail Route Debit Cards Containing Public Benefits - April 24, 2023

From at least August 2015 to May 2020, Toshell Hunter schemed to defraud Bank of America by using her position as a USPS mail carrier to steal mail containing California Employment Development Department (EDD) debit cards that contained unemployment insurances benefits. Hunter also stole debit cards containing Economic Impact Payments for federally issued monetary relief because of the COVID-19 pandemic, United States Treasury checks, and other mail containing personal identifying information related to victims assigned to Hunter's mail route.

Hunter would then give the stolen EDD and other cards to co-defendant Michalea Barksdale who then activated and fraudulently used them. Hunter provided Barksdale the stolen debit cards in exchange for future payments and gifts.

Hunter helped Barksdale make fraudulent and unauthorized cash withdrawals from 68 separate victims' accounts and stole approximately $204,812 from Bank of America. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

FBI Arrests Massachusetts Air National Guardsman In Probe Of Classified Document Leaks - April 13, 2023

FBI agents arrested Massachusetts Air National Guardsman Jack Douglas Teixeira at a home in North Dighton, Massachusetts, in connection with a trove of classified documents that have been leaked online in recent months.

Teixeira, who joined the Air National Guard in September 2019, held the highest-level security clearance granted by the federal government for top secret information.

Teixeira was most recently stationed at Otis Air National Guard Base as a member of the of 102nd Intelligence Wing. He was promoted to Airman 1st Class last July.

That New York Times report named Teixeira as the leader of a Discord group called "Thug Shaker Central" that consisted of roughly 20 to 30 young men.

Teixeira allegedly starting sharing classified documents with the private group in recent months, but the leaks gained wider attention after another member shared them in a public forum, according to the report.

Investigators don't believe that the case ends with Teixeira and are looking at other who may be involved, a source told Fox News. (Source)

2 Army Officers (Husband, Wife) Plead Guilty To The Theft Of Government Property Theft That Profited Them $2 Million+ - April 21, 2023

2 Army Officers (Husband, Wife) have been convicted in a multi-year activity involving the theft of more than $2 Million in government property. Chief Warrant Officer Three (CW3) Christopher Hammond pled guilty to theft / possession of government property and money laundering. His wife Major Heather Hammond was convicted for spending money laundering proceeds and aiding and abetting.

CW3 Hammond used his position to requisition government property intended for his unit at Ft. Bragg. The property was never logged into inventory at the base but was instead sold by Hammond to various individuals. In a two-year period, CW3 Hammond received at least $1.8 million in wire transfers related to the sales, which he deposited into bank accounts controlled by him and his wife. The investigation traced about 200 items sold by CW3 Hammond or held in his home as having been issued to Hammond's military unit.

Major Hammond knowingly allowed use of her bank accounts, even suggesting the use of her accounts so the money would not go into Chief Hammond's bank account. The fraud was uncovered when a supplier noticed that items procured under a government contract were being sent in for warranty repairs by a private individual. (Source)

U.S. Army Contracting Officer Pleads To Theft Of $490,000+ / Used Fund Vacations - April 3, 2023

Thomas Bouchard was the Contracting Officer in charge of the U.S. Army Natick Contracting Division, a full-service contracting organization for the Department of Defense.

In 2014, Bouchard used his long-standing relationship with Evolution Enterprise, Inc., a government contractor, to allegedly have Chantelle Boyd hired for a "no show" job as an assistant that specifically supported Bouchard. Boyd's position cost the Department of Defense more than $490,000 during her time at Evolution from 2014 to 2018, during which Boyd performed little if any useful function.

Bouchard and Boyd took numerous government-funded trips, ranging in duration from two to 15 days, under the guise that they were work related. This included 31 trips to Orlando, Fla., among other locations such as Clearwater Beach, Fla., and Stafford, Va., during which Boyd allegedly performed little if any work. For many of the trips, Bouchard and Boyd stayed in the same hotel room and spent time at the pool and Disney parks – all during business hours. In order to conceal the personal nature of the trips, Bouchard altered, created and approved false travel to reimburse the Boyd for out-of-pocket expenses. (Source)

Air National Guardsman Charged In Murder-For-Hire Scheme / Needed Money - April 14, 2023

Josiah Garcia needed money to support his family and in mid-February began searching online for contract mercenary jobs and came across the website www.rentahitman.com. Originally created in 2005 to advertise a cyber security startup company, the company failed and over the next decade it received many inquiries about murder-for-hire services. The website's administrator then converted the website to a parody site that contains false testimonials from those who have purported to use hit man services, and an intake form where people can request services. The website also has an option for someone to apply to work as a hired killer.

Garcia submitted an employment inquiry indicating that he was interested in obtaining employment as a hit man.

Garcia followed up on this initial request and submitted other identification documents and a resume, indicating he was an expert marksman and employed in the Air National Guard since July 2021. The resume also indicated that Garcia was nicknamed "Reaper" which was earned from military experience and marksmanship. Garcia continued to follow up with the website administrator indicating that he wanted to go to work as soon as possible.

An FBI undercover agent then began communicating with Garcia who subsequently agreed to kill an individual for $5,000. On Wednesday, Garcia met the undercover agent at a park in Hendersonville, Tennessee, and was provided with a target packet of a fictional individual, which included photographs and other information about the individual to be killed, and a down payment of $2,500. After agreeing to the terms of the murder arrangement, Garcia asked the agent if he needed to provide a photograph of the dead body. Garcia was then arrested by FBI agents, who in a subsequent search of his home, recovered an AR style rifle. (Source)

CRITICAL INFRASTRUCTURE

2023 Report States That Critical Infrastructure Leaders Are Concerned Over Insider Threat - April 20, 2023

Over a third (35%) of critical national infrastructure (CNI) security leaders believe the economic downturn is forcing employees to turn to data theft and sabotage, according to the Bridewell Consulting Report. (Source)

Overall, the number of employee sabotage incidents at CNI firms surged by 62% year-on-year, according to the report.

Bridewell Consulting polled 1025 individuals with responsibility for cybersecurity in UK and US CNI firms across the communications, utilities, finance, government and transport and aviation sectors.

Many believe the cost-of-living crisis may be driving insiders at these firms to do the bidding of cybercrime groups in return for a big pay-off.

Their suspicions are backed by hard evidence: the financial services sector was hit worse than any other industry sector studied for the report last year. Organizations in the vertical suffered on average 28 security incidents caused by employee sabotage over the previous 12 months, as well as 28 instances of data theft or misuse.

Challenging economic conditions are also putting pressure on CNI firms in other ways. Almost two-thirds (65%) of UK respondents said they had seen "some reduction" or a "significant reduction" in their cybersecurity budget, rising to 73% of US respondents.

The communications sector has been impacted the least by these cuts, with almost half (48%) claiming to have seen no change in security budgets. At the other end of the spectrum, the transport and aviation (73%) and utilities sectors (69%) experienced the greatest falls. Utilities also includes energy, oil and gas companies. (Source)

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

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

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

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

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

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

Lawson was responsible for recruiting more than 200 individuals to participate in this PPP and EIDL fraud scheme. Three of the individuals she recruited were active sheriff's deputies and one was a former U.S. Army military policeman. Lawson submitted PPP and EIDL applications seeking over $6 million in funds earmarked to save small businesses from the impacts of COVID-19.

She and her co-conspirators ultimately stole more than $3 Million. Lawson used a portion of these funds to purchase a $74,492 Mercedes Benz, a $13,500 Kawasaki motorcycle, $9000 worth of liposuction, and several other expensive items. (Source)

Former New York City Correction Officer Sentenced To Prison For Accepting $34,000+ In Bribes In Exchange for Smuggling Contraband Into Prison - April 25, 2023

Katrina Patterson accepted at least $34,090 in bribes from co-conspirators in exchange for Patterson's smuggling contraband into the Robert N. Davoren Center on Rikers Island for inmate (and co-defendant) Michael Ross. Ross, who was incarcerated on unrelated offenses, arranged for the bribes to be sent to Patterson.

The Department Of Correction subsequently located narcotics and cell phones in Ross' cell. Law enforcement also recovered Patterson's text messages, including messages where a co-conspirator told Patterson that some of the contraband would be "4 black joints in 1 paper," and Patterson responded, "it better be wrapped so many times I don't want to smell it." Patterson also discussed with her co-conspirator the need to delete their text messages. (Source)

STATE / CITY GOVERNMENTS / MAYORS

Former Idaho Transportation Department Employee Pleads Guilty To Receiving $38,000 In Bribes For Passing Scores On Commercial Driver's License Tests - April 3, 2023

Kelly Goodman worked for the Idaho Transportation Department as commercial driver's license (CDL) Skills Test Examiner.

Goodman engaged in a scheme to accept bribes in return for providing passing scores on Idaho CDL skills tests. Between December 2017 and May 2020, Goodman accepted numerous bribes in exchange for giving passing scores on Idaho CDL skills tests. During that time, Goodman received at least $38,000 in bribes in exchange for giving passing scores on Idaho CDL skills tests. (Source)

Former State Highway Patrol Inspector Admits Accepting $14,000+ In Cash Bribes - April 25, 2023

Larry Conrad pleaded guilty to one felony charge of using a facility in interstate commerce, a cellular telephone, to facilitate his bribery scheme. He admitted accepting a total of about $14,020 in individual bribes to falsify forms and approve inspections of vehicles that had been damaged and had salvage titles or were listed as "abandoned," even if he never saw the vehicle.

Conrad's primary duty was to perform motor vehicle inspections at the Missouri State Highway Patrol's Troop C facility in south St. Louis County. There is no fee for the inspections. If the vehicle passes, an inspector signs and certifies forms required for motor vehicle owners to apply for original Missouri Certificates of Title.

Conrad admitted accepting individual cash bribes ranging from $40 to $160 to pass vehicles. He often falsified certificates to indicate there was no apparent damage when there was visible damage to the vehicle being inspected.

On multiple occasions, Conrad took money for the inspection of vehicles that he never saw, including at least one that was not drivable.

Conrad communicated with the vehicle owners via text messages and cell phone conversations and had them place the cash bribes in the driver's side door pocket. Conrad would then take the money at the time he was to be performing the inspection. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

Former University Administrator Sentenced To Prison For Role In $155,000+ Wire Fraud Scheme - April 27, 2023

Brian Carroll was serving as the Executive Vice President of Southeastern University, a private university in Lakeland, Florida.

Carroll became involved in a project to redesign the website and digital brand of the university's President. Carroll conducted a self-dealing scheme to enrich himself by setting up an "anonymous" LLC based in New Mexico and setting up a bank account in the name of that LLC, both of which he controlled. The Board of Directors and President of Southeastern University were unaware of Carroll's involvement in this LLC.

The LLC that Carroll controlled then submitted a bid to the university to perform the web rebranding project for a total price of $185,000. Carroll recommended and promoted the acceptance of this contract, thereby causing the university to make a number of wire payments to that LLC for work done on the project. Unbeknownst to the university, Carroll's LLC contracted with an unrelated company based in New York to do the actual work on the project and create the new website.

This New York company charged Carroll's LLC $30,000 for the project. Carroll thus engineered a scheme to pay his LLC $185,000 for a project that, in reality, cost only $30,000 to perform. He thereby defrauded Southeastern University out of approximately $155,000. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

Former Union Financial Secretary Pleads Guilty To Stealing $143,000+ Of Union Funds - April 28, 2023

Brian Gerald was the Financial Secretary of United Steelworkers Local 13-189 Union.

Gerald was responsible for organizing Local 13-189's financial records, keeping an accounting of its income, and filing IRS forms and reports. Gerald was also responsible for maintaining Local 13-189's debit card in a safe location.

From January 2015 through September 2020, Gerald misused the union's debit card to make 493 ATM cash withdrawals totaling $107,387.90 in cash and fees. Gerald also misused the union's debit card to make payments for his personal accounts for a total of $36,589.41. Gerald misappropriated a total of $143,977.31 of union funds. (Source)

Former Union President Pleads Guilty To Embezzling $74,000+ From Union For Personal Use - April 19, 2023

James Boatman is the former President of the United Food and Commercial Workers (UFCW) Local 617 Union.

Botman embezzled and stole union funds for his personal use. The investigation revealed that Boatman from 2010 until 2019, set up a credit card in the Union's name, without authorization, and from at least May 2017 to

August 2019 used the card for personal expenses, including vacations to Florida, large repairs on his personal vehicle, and to pay for attorney representation for an unrelated matter. Boatman wrote checks from the Union funds to cover personal expenses and to pay himself for unauthorized lost time for periods of time Boatman claimed he was conducting Union business. Boatman pled guilty and agreed to pay $74,231.34 in restitution to the Union. (Source)

BANKING / FINANCIAL INSTITUTIONS

Former Bank Customer Service Representative Employee Pleads Guilty To Stealing $70,000+ From Customers' Accounts To Pay Her Bills & Others - April 3, 2023

In April 2022, Lladira Hernandez was hired by the bank as a Customer Service Representative.

She began stealing the bank account information for customers she helped over the phone and used it to pay bills for herself and her associates. This included mortgage payments, car payments, and phone bills. In August 2022, Hernandez transferred more than $45,000 from two customers' accounts into her own account and abruptly quit her job at the bank. She proceeded to withdraw that money from her account and was captured doing so on surveillance video.

Hernandez stole $70,000+ from multiple customers' accounts. (Source)

Mortgage Loan Officer Convicted Of Bank Fraud And Aggravated Identity Theft Charges Involving Forging Of Judges' Signatures - April 12, 2023

Ujaque Omayra, in her capacity as a licensed mortgage loan officer, created and executed a mortgage fraud scheme targeting the financial institution where she worked.

To ensure that otherwise unqualified borrowers were approved for mortgage loans, Ujaque falsified the borrowers' income by fabricating or inflating the amounts of their monthly child support payments on mortgage loan applications that she signed and certified to the financial institution's underwriting department. Ujaque created fictitious Final Judgments of Dissolution of Marriage and Final Orders Modifying Child Support that fraudulently represented that the borrowers were entitled to receive non-existent monthly child support payments. Ujaque then used the names of judges from the Circuit Court of the Ninth District of Florida and forged their signatures on the fabricated Final Judgments of Dissolution of Marriage or Final Orders Modifying Child Support.

Ujaque also created bogus Florida Department of Revenue Statements listing fraudulent monthly child support payments, as well as phony prepaid debit card statements listing fake borrower withdrawals of the non-existent monthly child support payments. In most cases, the borrowers did not, in fact, have the listed children and/or had never been married. Ujaque submitted bogus paperwork to the financial institution to support the false monthly income on the loan applications. Based on Ujaque's misrepresentations, the financial institution approved and funded the mortgage loans. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Tesla Workers Shared Sensitive Vehicle Camera Information With Other Workers - April 6, 2023

But between 2019 and 2022, groups of Tesla employees privately shared via an internal messaging system sometimes highly invasive videos and images recorded by customers' car cameras, according to interviews by Reuters with nine former employees.

Some of the recordings caught Tesla customers in embarrassing situations. One ex-employee described a video of a man approaching a vehicle completely naked.

Also shared: crashes and road-rage incidents. One crash video in 2021 showed a Tesla driving at high speed in a residential area hitting a child riding a bike, according to another ex-employee. The child flew in one direction, the bike in another. The video spread around a Tesla office in San Mateo, California, via private one-on-one chats, "like wildfire," the ex-employee said.

Other images were more mundane, such as pictures of dogs and funny road signs that employees made into memes by embellishing them with amusing captions or commentary, before posting them in private group chats. While some postings were only shared between two employees, others could be seen by scores of them, according to several ex-employees.

Tesla states in its online "Customer Privacy Notice" that its "camera recordings remain anonymous and are not linked to you or your vehicle." But seven former employees told Reuters the computer program they used at work could show the location of recordings, which potentially could reveal where a Tesla owner lived.

One ex-employee also said that some recordings appeared to have been made when cars were parked and turned off. Several years ago, Tesla would receive video recordings from its vehicles even when they were off, if owners gave consent. It has since stopped doing so.

"We could see inside people's garages and their private properties," said another former employee. "Let's say that a Tesla customer had something in their garage that was distinctive, you know, people would post those kinds of things."

To report this story, Reuters contacted more than 300 former Tesla employees who had worked at the company over the past nine years and were involved in developing its self-driving system. More than a dozen agreed to answer questions, all speaking on condition of anonymity.

Reuters wasn't able to obtain any of the shared videos or images, which ex-employees said they hadn't kept. The news agency also wasn't able to determine if the practice of sharing recordings, which occurred within some parts of Tesla as recently as last year, continues today or how widespread it was. Some former employees contacted said the only sharing they observed was for legitimate work purposes, such as seeking assistance from colleagues or supervisors. (Source)

Columbia Sportswear Sues Two Former Execs For Trade Secrets Theft - April 27, 2023

Columbia Sportswear Company (CSC) filed suit against two former executives in Oregon District Court for alleged theft of trade secrets. The two former employees resigned on the same day and joined Huk Gear, the fishing apparel brand owned by Marolina Outdoor, Inc.

The lawsuit contends that William Ferreira, Columbia's former Director of Global Merchandising for Columbia's PFG-PHG, youth, accessories, headwear, and equipment categories, and Dean Rurak, who served as SVP and Chief Product Officer for Columbia Sportswear, misappropriated confidential documents. Ferreira joined Columbia in July 2004, and Rurak joined the company in July 2008. Both resigned on October 28, 2022. (Source)

CHINESE ESPIONAGE TARGETING U.S. COMPANIES / UNIVERSITY TRADE SECRETS

8 Chinese Government Officials Charged With Directing Employee Of U.S. Telecommunications Company To Remove Chinese Dissidents From Company's Platform - April 17, 2023

10 defendants, including a former executive of a U.S. telecommunications company who worked in the People's Republic of China (PRC), 6 officers of the PRC Ministry of Public Security (MPS), 2 officials with the Cyberspace Administration of China (CAC), and 1 other civilian with conspiracy to commit interstate harassment and unlawful conspiracy to transfer means of identification. All the defendants are believed to reside in the PRC and remain at large. (Source)

Former Harvard University Professor Sentenced To Prison For Lying About His Affiliation China's Thousand Talents Program - April 26, 2023

The former Chair of Harvard University's Chemistry and Chemical Biology Department (Dr. Charles Lieber) was sentenced today in federal court in Boston for lying to federal authorities about his affiliation with People's Republic of China's Thousand Talents Program and the Wuhan University of Technology (WUT) in Wuhan, China.

Lieber served as the Principal Investigator of the Lieber Research Group at Harvard University, which between 2008 and 2019 conducted more than $15 million in research sponsored by various U.S. Government agencies, including the U.S. Department of Defense ("DOD") and the National Institutes of Health ("NIH"). Unbeknownst to his employer, Harvard University, Lieber became a "Strategic Scientist" at WUT and, later, a contractual participant in China's Thousand Talents Plan from at least 2012 through 2015.

Lieber earned income from WUT in the form of salary and other payments made to him pursuant to his Thousand Talents contract. (Source)

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

Former Physician's Assistant Sentenced To Prison For Health Care Fraud After Posing As A Licensed Practitioner - April 18, 2023

In September 2019 Theresa Pickering was hired as a Licensed Physician's Assistant at a family practice in Norcross, Georgia.

But Pickering was not a licensed physician's assistant in Georgia at that time, nor had she been a licensed physician's assistant in any state since March 2014. After Pickering served a prison sentence for a 2015 fraud and narcotics case related to her illegal practice as a physician's assistant in the State of Mississippi, Pickering relocated to Georgia and again obtained employment as a licensed physician's assistant at the Norcross-based family practice.

While employed at the practice, Pickering treated patients, diagnosed illnesses, ordered diagnostic tests and lab work, and handled sick visits and prescribed drugs to patients – none of which was authorized by law based on her lack of licensure and exclusion from federal health care programs. Pickering also issued prescriptions, including prescriptions for controlled substances, in the name of Doctor 1, a physician contracted by the practice, and without Doctor 1's permission. Pickering caused the practice to submit at least approximately $147,000 in fraudulent claims for reimbursement to Medicare and numerous private insurance companies. (Source)

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

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

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

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

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

The pair are accused of having used the facade of a joint-venture and $2.7 billion in assets "which in reality it did not possess" to lure $1 Billion in financing from 1MDB, according to Swiss prosecutors.

The two opened Swiss bank accounts to receive the money, and then used the proceeds to acquire luxury properties in London and Switzerland, as well as jewellery and funds "to maintain a lavish lifestyle," the prosecutors said.

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

Former Apple Employee Sentenced To Prison For Conspiracy To Defraud Apple Of $19 Million+ - April 26, 2023

Dhirendra Prasad was sentenced to serve three years in prison and ordered to pay $19,270,683 in restitution for conspiring to defraud Apple, Inc., of millions of dollars and for related tax crimes.

The criminal conduct in this case centered around Prasad's employment at Apple from December 2008 through December 2018. For most of that time, he was a "buyer" in Apple's Global Service Supply Chain. It was Prasad's job as an Apple buyer to facilitate the process through which Apple bought parts to perform warranty repairs on older devices. Prasad exploited his position and conspired with two separate Apple vendors to defraud Apple by taking kickbacks, stealing parts, inflating invoices, and causing Apple to pay for items and services it never received – resulting in a loss to Apple of more than $17,000,000. In addition to engaging in two separate criminal conspiracies with Apple vendors, Prasad also acknowledged that he evaded tax on the proceeds of his schemes.

According to the government's sentencing memorandum, by virtue of his position at Apple Prasad was given substantial discretion to make autonomous decisions to benefit his employer. Prasad betrayed this trust, and abused his power to enrich himself at his employer's expense all while accepting hundreds-of-thousands of dollars' worth of compensation from Apple in the form of salary and bonuses. Additionally, Prasad used his insider information regarding the company's fraud-detection techniques to design his criminal schemes to avoid detection. (Source)

Financial Controller Sentenced To Prison For Embezzling $3 Million+ From 2 Companies That Employed Her - April 17, 2023

Rosalba Meza worked for 2 companies as a Financial Controller

From May 2017 through the end of 2019, Meza made unauthorized transfers totaling approximately $3,071,880 to her own bank accounts from accounts belonging to Trilogy Plumbing Inc. and a related back-office support company called Matrix Management LLC.

Meza held various positions at these companies since 2003 and was entrusted with access to and control of the companies' financial and banking information. In her role, Meza whose annual salary was approximately $65,000 oversaw and handled the companies' daily financial activities, including banking, bookkeeping and preparation of financial statements. She also had the authority to access the companies' bank accounts for the purpose of making authorized electronic payments on the companies' behalf.

Meza used her knowledge of the companies' accounting software to intentionally falsify their accounting records.

She misrepresented the amounts in the companies' various accounts to conceal the unauthorized transfers and falsely show the companies' accounts were balanced. For example, Meza falsely recorded some unauthorized transfers as business expenses, when in fact these amounts were payments to herself.

In February 2019, Meza told executives their companies did not have funds to meet payroll obligations and failed to inform the executives that she had been embezzling from the companies.

Several months later, while the companies were the subject of an IRS enforcement action because of unpaid payroll taxes, Meza falsely told the executives that she did not pay the quarterly payroll taxes because she instead had used those funds to pay employees.

Once Meza transferred the funds to her accounts, she used the stolen money on personal expenses, withdrew a large amount in cash, wired a significant amount to a family member-owned bank account in Mexico and made other transfers of the illicitly obtained funds to family and friends. The scheme lasted until January 2020, when Trilogy and Matrix fired Meza. (Source)

Former Account Manager Admits To Embezzling $3 Million+ For 10 Years - April 27, 2023

Judy Green admitted to embezzling over $3 million from her employer for approximately 10 years.

Green worked as an account manager for a Houston-based building and maintenance supply company. As part of the scheme, she submitted fraudulent invoices to induce payment from the company and pocketed the funds for personal expenses. Ultimately, the scheme was uncovered 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. (Source)

Construction Company Owner Sentenced To Prison For Bid Rigging And Paying Department of Transportation Official $1 Million In Bribes - April 17, 2023

Bill Miller engaged in a conspiracy from April 2015 through as late as December 2019. As part of the conspiracy, Miller recruited others to submit sham bids on Caltrans contracts, including co-conspirator William Opp, a former business partner who pleaded guilty in the case on Oct. 3, 2022.

In addition to pleading guilty to bid rigging, Miller also pleaded guilty to paying bribes to Keith Yong, the former Caltrans contract manager who managed the contracts involved on behalf of Caltrans, a California state agency that receives significant federal funding. On April 11, 2022, Yong pleaded guilty for his role in the bid-rigging and bribery scheme. Yong received the bribes in the form of cash payments, wine, furniture and remodeling services on his home. The total value of the bribes that Miller paid to Yong was nearly $1 Million. (Source)

Former Payroll Manager For Chicago Museum Admits To Misappropriating $2 Million+ - April 12, 2023

From 2007 to 2020, Michael Maurello siphoned money from the museum's payroll account to his personal bank accounts by falsely designating the payments as legitimate compensation to other employees.

Maurello admitted that he kept spreadsheets and notes to track the misappropriated money so that he could later make reversals within the payroll system to hide his fraudulent scheme. When the museum's assistant controller asked Maurello in January 2020 about one of the payments, Maurello falsely stated that the transaction had been a test of the payroll system. Maurello then edited and altered a report from the payroll system to conceal information about the misappropriated funds. (Source)

Former Bookkeeper Sentenced To Prison For Stealing $930,000 From 2 Employers - April 24, 2023
Susan Sears served as the Bookkeeper for Shapery Enterprises from July 2018 to November 2019.

Sears admitted that she opened a personal American Express credit card in the name of a family member, obtained American Express cards for herself and family members, and used Shapery Enterprises' bank account to pay the personal American Express account. Sears made the payments appear to be legitimate business expenses by entering "S. Sharpery," which is one letter off from the CEO's last name of Shapery.

Sears also issued herself unauthorized checks and falsified entries in the business' accounting programs. In total, Sears stole more than $765,000 from Shapery Enterprises. Since American Express reimbursed Shapery Enterprises $674,673.93, Sears admitted that the loss to American Express was $674,673.93.

After Sears was fired from Shapery Enterprises in November 2019 and the government notified her that she was under investigation for wire fraud, Sears was employed by Hope Campbell Realty as its Bookkeeper from February 2021 to November 2021. Sears again abused her position of trust and issued herself and her family members unauthorized checks. Sears also falsified entries in Hope Campbell Realty's accounting programs to make it appear that the checks were for legitimate business purposes. Between March 2021 and November 2021, Sears stole nearly $165,000 from Hope Campbell Realty. (Source)

Former Bookkeeper Charged With Embezzeling $109,000+ - April 17,2023
From January 2015 to June 2018, Mary Katicich was employed as a bookkeeper with Company A based in Belle Chase, Louisiana.

During this timeframe, Katicich stole funds from Company A's bank accounts without permission or authorization.

To enact this scheme, Katicich executed electronic transfers from Company A to her business and personal bank accounts via ACH deposits and payroll check deposits in amounts exceeding her authorized annual salary.

To conceal her embezzlement scheme, Katicich failed to report to the IRS funds that she received from Company A, resulting in a total tax loss to the IRS of approximately $109,664. (Source)

Architectural Design And Construction Management Firm Vice President Bribes 2 City Officials $40,000+ For Work
From 1984 to 2018, PRAD Group was an architectural, design, and construction management firm headquartered in Atlanta, Georgia, that performed services for the City of Atlanta and DeKalb County, Georgia. Jeff Jafari served as PRAD Group's Executive Vice President and oversaw PRAD Group's finances.

Jafari has pleaded guilty to paying bribe money to 2 City of Atlanta officials in exchange for steering city business worth millions of dollars to his company, to paying bribes to a former Dekalb County official in an attempt to obtain county contracts, and to evading more than $1.5 million in taxes.

From January 2003 to February 2017, Adam Smith served as the Chief Procurement Officer for the City of Atlanta. From that position, Smith supervised the City of Atlanta's purchasing activities and its expenditure of billions of dollars of public money. From April 2011 to May 2016, Jo Ann Macrina served as the City of Atlanta's Commissioner of the Department of Watershed Management. As Watershed's Commissioner, Macrina held a cabinet-level position from which she managed the City's drinking water and wastewater systems and was responsible for an annual budget exceeding $500 million.

Jafari gave Smith and Macrina cash and other items of value to obtain business with the City of Atlanta. For years, Jafari met privately with Smith on multiple occasions, frequently at local restaurants. During these meetings, Jafari and Smith discussed City of Atlanta procurement projects, bids, and solicitations. Often at the time of these meetings, Jafari was actively seeking additional work and / or assistance with ongoing City projects. Jafari paid Smith $1,000 in cash in the bathroom of the restaurant after most of the meetings. In return for these bribe payments, Jafari expected Smith to use his position and power to assist Jafari with contracting / procurement with the City of Atlanta. From at least 2014 to January 2017, Jafari paid Smith more than $40,000 in cash with the intent to influence Smith in his role as the City of Atlanta's Chief Procurement Officer. (Source)

3 Current / Former Executives For Ship Builder Charged With Accounting Fraud - April 1, 2023

3 current and former executives of a shipbuilder that constructs vessels for the U.S. Navy and Coast Guard have been indicted on accounting fraud charges accusing them of falsely inflating the company's reported earnings, federal prosecutors said.

Craig Perciavalle, Joseph Runkel, and William Adams are accused of misleading shareholders and investors. They worked for Austal USA.

Austal USA LLC is a subsidiary of Australia-based Austal Limited and builds littoral combat ships for the Navy. The ships are designed to operate in shallow coastal waters.

Perciavalle resigned as Austal USA's president in 2021 following an investigation by federal and Australian authorities into practices dating back more than four years, the company said at the time. Adams is the former Director of the Littoral Combat Ships Program, according to the SEC. Runkel is the Director of Financial Analysis.

Prosecutors alleged the 3 men manipulated an accounting metric to hide growing costs in order to maintain and increase the share price of Austal Limited's stock, hurting U.S. investors. (Source)

EMPLOYEES' WHO EMBEZZLE / STEAL MONEY FOR PERSONAL ENRICHMET AND TO LIVE ENHANCED LIFESTYLE

Former State Employee Sentenced To Prison For Role In $2 Million Scheme To Defraud The Office of AIDS / Used Funds For Personal Use - April 20, 2023

Between December 2017 and November 2018, Yvonne Gaide participated in a fraud scheme along with Schenelle Flores and Christine Iwamoto both former Office of AIDS employees.
In total, the participants in the fraud scheme obtained at least $2 million in personal benefits, including cash and purchased items.

Flores directed a state contractor to make payments allegedly on behalf of the Office of AIDS and to charge those payments to the state. In reality, those payments benefitted Gaide, Flores, Iwamoto, and others personally rather than the Office of AIDS. For example, Gaide, Flores, and Iwamoto caused the contractor to pay for personal expenses on its debit cards, order gift cards for personal use, and pay false invoices to shell companies for services allegedly provided to the Office of AIDS. This included, among other things, $450,000 in phony invoices submitted by Iwamoto for a shell company that she had created to defraud the state, which Gaide and Flores then helped ensure would be paid. After the invoices were paid, Iwamoto shared the proceeds with Gaide by meeting in person to give Gaide cash, as well as giving Gaide blank checks that she could write out of the phony company's bank account. (Source)

Former Company Controller Pleads Guilty To Embezzling $1.67 Million / Used Funds For Gambling & Personal Expenses - April 18, 2023

Constance Stobert worked as a Controller for a company called Mechanical Operations Company (MOC) from 1994 until July 2021.

Between January 2014 and July 2018, Stobert embezzled at least $1,678,893 in MOC's assets to fund her gambling habit and to pay for her personal expenses. Among other things, Stobert wrote checks from MOC's business banking accounts to make personal credit card payments and used MOC's credit cards to withdraw cash at ATMs in casinos located in Pittsburgh and Las Vegas.

Stobert also admitted that, during the tax years 2016, 2017, 2018 and 2019, she willfully and knowingly filed false tax returns, in which she failed to report the money she embezzled from MOC, resulting in a tax loss to the government of $545,990. (Source)

Former Office Administrator / Bookkeeper Sentenced To Prison For Embezzling $286,000+ From Employer For Personal Use (Clothing, Vacations, Pay Credit Card Bills, Etc._ - April 28, 2023

Kelley Kann was employed for several years as an Office Administrator and Bookkeeper for a business. Kann's role, a position of financial trust, granted her access to the company's financial information and payment mechanisms, allowing her to conduct financial transactions for the company and its affiliated businesses.

In July 2018, Kann fraudulently obtained Capital One credit cards using the name, date of birth, and social security number of the spouse of the company's owner. On recorded phone calls that Kann made to Capital One's customer service line, Kann falsely represented herself as the spouse and provided the spouse's personal identifiable information.

Between July 2018 and May 2021, Kann used the Capital One credit cards to make hundreds of unauthorized purchases of goods and services for her own personal benefit and without the company's authorization.

Kann's fraudulent purchases included, among other things, clothing, electronics, food, furniture, streaming services, utilities payments, and vacations for herself and a personal associate. Kann then paid the credit card bills via dozens of unauthorized transfers from the bank accounts of the company and its affiliated businesses, causing a total loss of $286,307.73.

In May 2021, when the company's owner confronted Kann about the theft, Kann wrote a handwritten statement admitting to stealing what she then claimed was only $20,000 and vowing to repay the money. Kann provided the owner with doctored bank statements that did not accurately reflect account balances and transactions. Kann later stopped reporting for work and did not repay any money. (Source)

Former Administrative Manager For Public Works Department Pleads Guilty To Wire Fraud / Identity Theft - Making $150,000 In Purchases For Herself - April 17, 2023

Allison Donaldson was employed as an Administrative Manager for the Public Works Department, from 2005 until 2022, and had access to credit card information for the department.

Starting in February 2020 and continuing until February 2022, Donaldson knowingly defrauded the City of Covington, by using employee credit cards and making over $150,000 in purchases for herself and her home. Some of the purchases listed in the plea agreement include repairs for a Mercedes Benz, a Louis Vuitton agenda, a Chanel tote, Crate & Barrel furniture, and a remodel to her master bedroom and garage. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

No Incidents To Report

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

No Incidents To Report

THEFT OF ORGANIZATIONS ASSESTS

No Incidents To Report

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG RELATED INCIDENTS

Assistant Director Of Nursing At Medical Rehabilitation Center Pleads Guilty To Tampering With Patient Medications / Using For Her Personal Use - April 11, 2023

Sarah Diamond was employed as the Assistant Director of Nursing at a Chicago-area medical rehabilitation center where she was responsible for dispensing medications to patients.

In July and August 2021, Diamond removed morphine from bottles prescribed to patients and replaced it with another liquid, knowing the diluted substance would be dispensed to the patients.

Diamond diluted a bottle of morphine intended for one of the patients, so that it contained only approximately 26% of the declared amount of morphine; and diluted a bottle of morphine intended for another patient so that it contained only approximately 53% of the declared amount of morphine. Diamond then administered liquid morphine shots to these patients using the diluted bottles, withholding the remainder of the pain medication intended for them for her own personal use. In total, Diamond removed liquid morphine intended for use by at least five patients at the rehabilitation center, each of whom had been prescribed liquid morphine to manage their pain. (Source)

Former Emergency Department Nurse Sentenced To Prison For Stealing Pain Medication For Herself And Them Injecting Patients With Saline - April 12, 2023

From October 1, 2018, to February 18, 2020, Jennifer Adams repeatedly tampered with vials of injectable pain medications, including fentanyl, morphine, hydromorphone, and ketamine, while employed as a registered nurse in the emergency department at Franciscan Health in Crawfordsville, Indiana.

Using an automated medication dispensing machine, Adams gained access to the medications without authorization and used them herself. To conceal her scheme, she refilled the vials of medicine with saline solution and super glued the lids back on.

Adams used the saline solution on thirty to forty unknowing patients who had been admitted to the emergency department and were in need of pain relief. The investigation found that Adams tampered with between two and seven vials of medicine during each shift that she worked. (Source)

Former Nurse Working At Surgical Center Pleads Guilty To Stealing Fentanyl For Personal Use - April 13, 2023

From approximately February 28 to April 18, 2022, Catherine Dunton, a Florida licensed Registered Nurse (RN), worked at an outpatient surgical center in Jensen Beach, Martin County, Fla. as a circulating nurse.

While working at the center, Dunton took vials of fentanyl, a narcotic painkiller in liquid form, and self-administered it by injection. To avoid detection, she replaced the fentanyl from nearly 450 vials with saline solution, and then returned the adulterated vials to the center for use during outpatient surgical procedures. (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 COMPANY TO CEASE OPERATIONS

No Incidents To Report

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'

Bank Employee Who Killed 5 Employees Was Told He Was Going To Be Fired - April 11, 2023

Authorities in Louisville, Kentucky, say they are still working to piece together details of Monday morning's mass shooting that left 5 people dead at a downtown bank, but a picture has started to emerge of the shooter who waa a 25-year-old bank employee.

Police identified the shooter as Connor Sturgeon, who they say livestreamed his killing of 5 Old National Bank employees. Sturgeon started working at Old National Bank as an intern in 2018, where he most recently worked as a syndications associate and portfolio banker.

Sturgeon worked at Old National Bank, a regional bank headquartered in Indiana. He was recently told he was going to be fired, according to CNN, citing a source with knowledge of the investigation. He left a note before the attack addressed to his parents and a friend telling them he was going to shoot up the bank.

People who knew Sturgeon told news outlets they did not see any red flags in his behavior, with former classmates describing him as a star athlete who was popular at Floyd Central High School in Floyds Knobs, Indiana. (Source)

Fired Restaurant Employee Sentenced To Prison For Molotov Cocktail Attack On Restaurant - April 19, 2023

Rashaad Cotton is a disgruntled former employee of a St. Charles, Missouri restaurant. He attacked it with Molotov cocktails.

On the evening of April 30, 2021, Cotton first threw a Molotov cocktail on a residential street in a suburban area in St. Charles. Twenty minutes later, he threw another on the northeast side of the Sauce on the Side restaurant on Beale Street and one near the front door.

A juvenile female with Cotton threw a Molotov cocktail at a patio area. The restaurant was open and serving customers. The pair then ran back to Cotton's vehicle and fled, but were arrested after they crashed.

Cotton told police that he had been fired from the restaurant the night before and wanted to scare people. (Source)

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)

EMPLOYEES' WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

Former Bank President Found Guilty Of $1 BILLION Of Fraud Resulting In Failure Of Bank - February 10, 2023

A federal jury has returned a verdict of guilty on all 46 counts against former First NBC Bank President and CEO Ashton J. Ryan, Jr. and not guilty on all 7 counts against former First NBC Bank Senior Vice President Fred V. Beebe.

From 2006 through April 2017, Ryan and others conspired to defraud First NBC Bank through a variety of schemes. Ryan was the President and CEO of the Bank for most of its existence. Ryan and others, conspired to defraud First NBC Bank by disguising the true financial status of certain borrowers and their troubled loans, concealing the true financial condition of the Bank from the Board of Directors, auditors, and examiners.

When members of the Board or the Bank's outside auditors or examiners asked about loans to these borrowers, Ryan and others made false statements about the borrowers and their loans, omitting the truth about the borrowers' inability to pay their debts without getting new loans. As a result, the balance on these borrowers' loans continued to grow resulting, ultimately, in the failure of First NBC. The Bank's failure cost the Federal Deposit Insurance Corporation's deposit insurance fund slightly under $1 billion. (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)

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

Information Technology Professional Pleads Guility 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

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

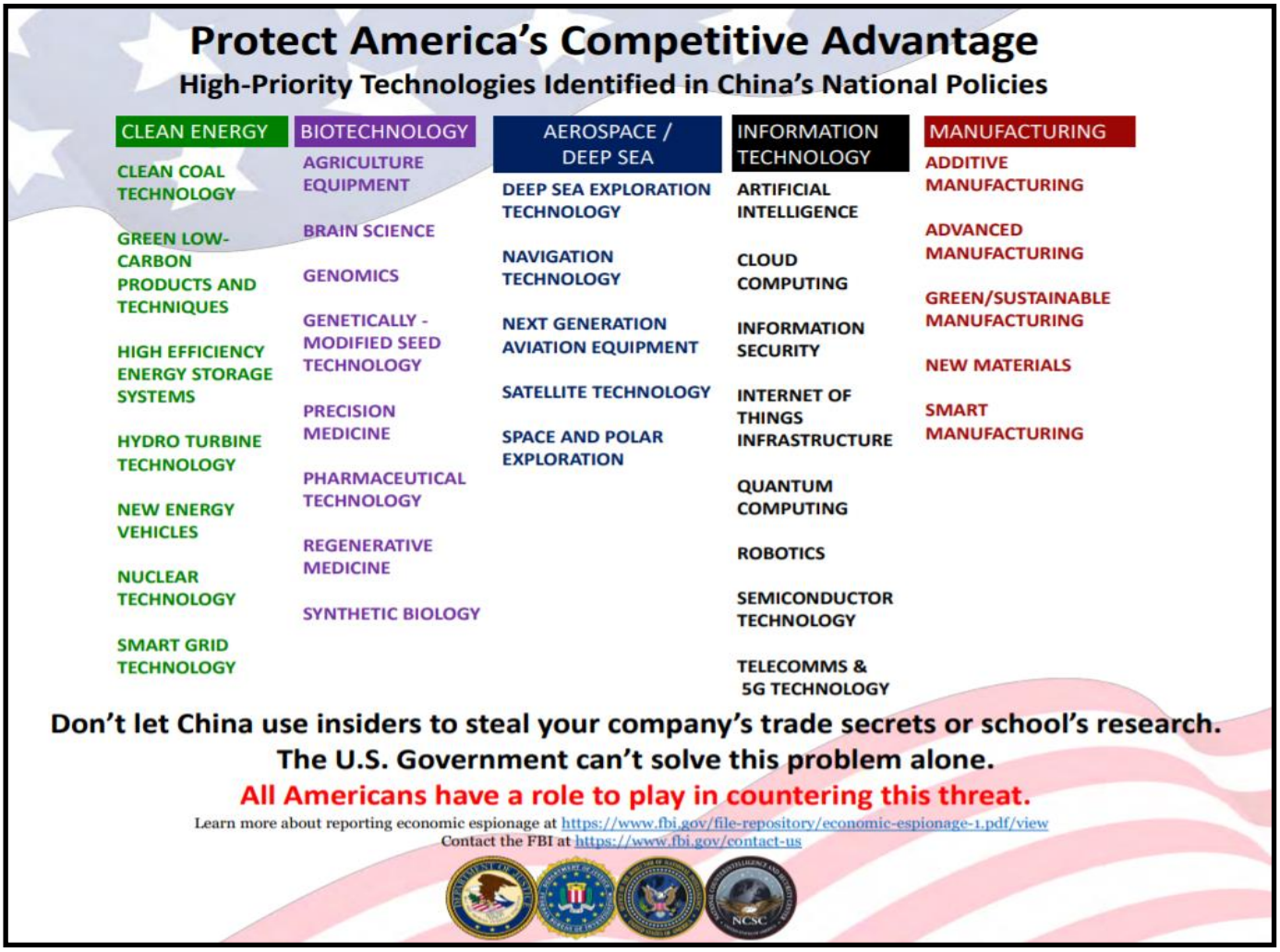
WORKPLACE VIOLENCE TODAY E-MAGAZINE
https://www.workplaceviolence911.com/node/994

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

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**4,400+ 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 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

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 due to the COVID outbreak. We are working on resuming meetings in the later part of 2021, and looking at holding the ITS&E in 2022.

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.insiderthreatdefense.us / james.henderson@insiderthreatdefense.us
www.nationalinsiderthreatsig.org / jimhenderson@nationalinsiderthreatsig.org