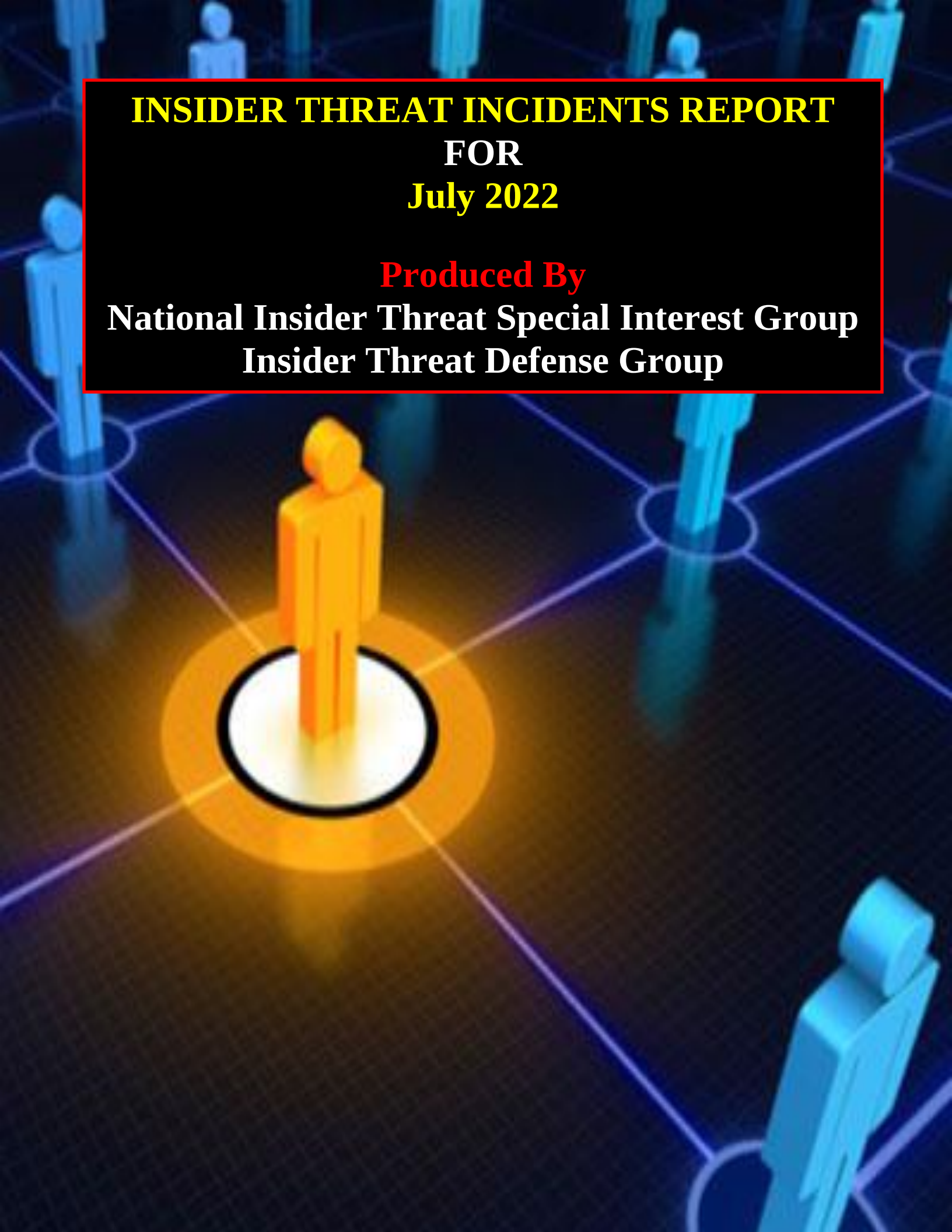


INSIDER THREAT INCIDENTS REPORT
FOR
July 2022

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 **3,900+** 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 2020 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 17 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.

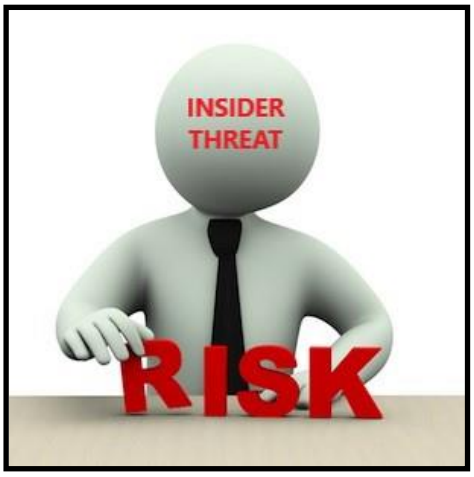
TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

- ☐ Non-Malicious But Damaging Insiders (Un-Trained, Careless, Negligent, Opportunist, Job Jumpers, Etc.)
- ☐ Disgruntled Employees Transforming To Insider Threats
- ☐ Theft Of Organizations Assets
- ☐ 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 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

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 JULY 2022

FOREIGN GOVERNMENT INSIDER THREAT INCIDENTS

2 Former Government Conttactor Workers Suspected Of Breaking Into The Spain Radioactivity Alert System Computer Network & Disabling Sensors - July 28, 2022

Spanish police have arrested two former government contractors, accusing them of a network breach on the nation's system for monitoring for dangerous levels of nuclear radiation. The alleged cybercriminals were once the people charged with maintaining and repairing that very detection network.

In spring of 2021, the former employees / now hackers broke into the country's radioactivity alert system, or RAR, which is a mesh network of 800 gamma radiation detection sensors stationed throughout the country. RAR, which is maintained by Spain's Directorate-General for Civil Protection and Emergencies (DGPCE), allows the government to monitor for abnormally high radioactivity levels at distributed geographical locations throughout the country. It was designed to protect against the kind of meltdowns that happened at Chernobyl.

The network intrusion which took place between March and June 2021, disrupted roughly a third of the sensors, leading to widespread failure within the network. For two months, the hackers attacked more than 300 sensors among the 800 existing ones, causing the failure of their connection with the control center and thus reducing the detection capacity of the network. (Source)

U.S. GOVERNMENT

No Incidents To Report

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Former CIA Software Engineer Convicted In Biggest Theft Ever Of CIA Secrets - July 14, 2022

Joshua Schulte was a CIA Programmer with access to some of the country's most valuable intelligence-gathering cyber tools used to battle terrorist organizations and other malign influences around the globe.

When Schulte began to harbor resentment toward the CIA, he covertly collected those tools and provided them to WikiLeaks, making some of our most critical intelligence tools known to the public, and our adversaries. Moreover, Schulte was aware that the collateral damage of his retribution could pose an extraordinary threat to this nation if made public, rendering them essentially useless, having a devastating effect on our intelligence community by providing critical intelligence to those who wish to do us harm. Today, Schulte has been convicted for one of the most brazen and damaging acts of espionage in American history. (Source)

Former U.S. Army Contracting Officer Pleads Guilty To Defrauding Government Of More Than $490,000 / Used Funds For 31 Vacations - July 7, 2022

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 allegedly performed little if any useful function.

Bouchard and allegedly 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, allegedly, 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)

STATE / CITY GOVERNMENTS / SCHOOL SYSTEMS / UNIVERSITIES

Former School Superintendent & 3 Others Sentenced To Prison For $2.8 Million+ Virtual Education Scheme / Used For For Personal Use - July 25, 2022

Former Superintendent of the Athens City Schools District, William Holladay was sentenced to 60 months in prison and ordered to pay $2,865,948.60 in restitution to Alabama State Department of Education (ALSDE).

During the same hearing, Gregory Corkren received a sentence of 22 months' imprisonment and was ordered to pay $1,303,514.28 in restitution to ALDSE.

David Tutt was also sentenced today to 24 months in prison and ordered to pay a fine of $15,000.00, plus $258,920.04 in restitution to ALDSE.

Thomas Sisk, formerly the Superintendent of the Limestone County School District, was sentenced to 18 months in prison and ordered to pay a fine of $15,000.00 and restitution in the amount of $13,000.00 to ALDSE.

All four of the above individuals had previously pleaded guilty to conspiring to fraudulently enroll students in public virtual schools and then falsely reporting those students to ALDSE. As a result of this conduct, districts received payments from Alabama's Education Trust Fund as if the students actually attended public schools. The various defendants then received, for their own personal use, portions of the state money. The defendants skimmed the state money through direct cash payments and payments to third-party contractors owned by the various co-conspirators. Corkren also pleaded guilty to aggravated identity theft. (Source)

Former School District Employee Pleads Guilty To Embezzling $250,000 - July 12, 2022

Terry Sanders was the former DeSoto ISD Director of Energy Management.

Sanders admitted he used a school district credit card to make 30 payments worth $255,100 to an outside company. The owner of the company then kicked back a portion of each payment, totaling approximately $100,000, to Mr. Sanders.

Sanders admitted that the company never performed any work for the school district, nor was the company an approved vendor with a contract with the district.

He also admitted that in order to test oversight of the card, he used the card to make seven payments worth $17,466 to pay a fictitious vendor tied to his own bank account. (Source)

Community College Director Sentenced To Prison For Stealing $230,000 Of Student Financial Aid Funds Over 6 Years / Used Funds For Family Members - July 19, 2022

From 2006 through 2017, Kiesha Pope, was the Director of Financial Aid at J. Sargeant Reynolds Community College (Reynolds), a public community college servicing the greater Richmond area.

From 2011 through 2017, Pope was involved in a scheme to defraud the Department of Education, the Commonwealth of Virginia, and Reynolds of educational funds. Pope used her financial aid office access to manufacture or boost financial aid eligibility for individuals, often her family members, who were not in fact eligible for financial aid. Thereafter, Pope directed at least four such co-conspirators to send her the majority of these financial aid funds. Pope spent financial aid funds on her personal expenses, such as a vacation on Disney Cruise Line, retail shopping, and expenses for her daughter.

To execute the scheme, Pope fraudulently overrode Reynolds' internal automated controls to manually place her co-conspirators in a status that guaranteed their continued receipt of financial aid funds. For instance, Pope used her access to the Reynolds financial aid systems to procure financial aid for her son from 2011 through 2017, knowing very well that her son was not attending Reynolds. In another instance, Pope procured financial aid for her ex-fiancé while that individual - a purported student at Reynolds - was actually serving a term of incarceration. (Source)

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

2 DHS Employees Workers Charged In Chinese Spying Scheme - July 7, 2022

U.S. prosecutors charged two men tied to the U.S. Department of Homeland Security (DHS) as part of what federal law enforcement officials have called a "transnational repression scheme" on behalf of the Chinese government to spy on and harass dissidents living in the United States.

The two men charged were Craig Miller, who has worked as a DHS Deportation Officer for 15 years in Minnesota, and Derrick Taylor, a retired DHS law enforcement agent now working as a private investigator in California.

A grand jury returned an indictment charging the two men and three others with crimes committed while acting as alleged Chinese agents. (Source)

Former Customs & Border Protection (CBP) Officer Sentenced To Prison For Taking Bribes To Allow Contraband Into U.S. - July 27, 2022

Simon Medina was a CBP Officer.

He admitted that between May 25 and Aug. 6, 2020, he allowed several individuals to enter the United States with contraband in their vehicles on approximately 20 occasions. Although not assigned to the entry lanes at the Laredo Port of Entry, Medina would open a lane and allow his co-conspirators to pass through without inspecting their cargo. Medina also accepted gratuities from his partners. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

Former Church Bookkeeper Pleads Guilty To Embezzling $175,000+ From Church - July 22, 2022

Anitia Hobdy pled guilty to wire fraud, stemming from fraudulent charges made from First Baptist Church of LaPlace.

Hobdy conducted the wire fraud scheme from 2015 through 2021. Hobdy worked as a Bookkeeper for a church's daycare and embezzled over $175,000 from church accounts during that period. (Source)

BANKING / FINANCIAL INSTITUTIONS

Former Bank Branch Manager Charged With Stealing $1 Million+ From Elderly Customers - July 11, 2022

Brian Davie worked for Wells Fargo from March of 2014 until he was fired in June 2019.

Davie used his position as a manager at the branch to conduct unauthorized transactions. Davie had access to customer files containing information about bank account balances, as well as examples of customer signatures. Davie used this knowledge to forge signatures on cashier's checks, withdrawal slips and other bank forms. Davie hid his criminal activity by repeatedly exchanging cashier's checks until they were small enough to cash without triggering banking reporting requirements.

Davie continued undetected because he stole from elderly customers who might be less likely to closely monitor their account balances. Some of Davie's victims had dementia, or had limited English skills and did not understand banking transactions.

Davie deposited some of the stolen money in an account he created in the name of a relative's business. He made some of the cashier's checks payable to that relative or to the business account he created. Much of the money was withdrawn as cash. Davie stole over $1 million. (Source)

TRADE UNIONS

Former Union Officer Pleads Guilty In Role To Embezzling $500,000+ / Used Funds For Parties, Trips, Furniture, Etc. - July 1, 202

Attia Little was the Operations Manager of the Property Services Division of the Service Employees International Union (SEIU). As part of her duties, she managed administrative support, booked reservations for SEIU employees, and paid vendor invoices for union-related purchases. She had a work-issued credit card and access to third-party discount travel booking platforms that were to be used for union business only.

Melba Norris, was a close associate of Little's, and had no affiliation with the union. between November 2015 and October 2017, Little used her access to the credit card and travel booking platforms to embezzle approximately $503,600 from SEIU. In total, she kept approximately $460,900 in SEIU funds for herself, and Norris kept approximately $42,700.

Little used the SEIU credit card to purchase personal items, including purchases for a baby, personal parties hosted at her residence, personal travel, furniture, watches, clothing, and video games. She also used the credit card to purchase gift cards for personal use. Little also used the credit card to pay funds to a company that she created and companies created and controlled by Norris, even though no work was performed. (Source)

Former Financial Secretary - Treasurer For United Auto Workers Union Sentenced To Prison For Embezzling $2 Million+ To Purchase Vehicles, Firearms & Gamble - July 27, 2022

Between 2011 and 2021, Timothy Edmunds served as the Financial Secretary-Treasurer of union Local 412 of the International Union, United Automobile, Aerospace, and Agricultural headquartered in Warren, Michigan.

Edmunds systematically drained the Local 412 accounts of $2.2 million by (1) Using Local 412 debit cards for over $142,000 in personal purchases, (2) Cashing Local 412 checks worth $170,000 into accounts he personally controlled, and (3) Transferring $1.5 million from Local 412 accounts into accounts that he personally controlled. Edmunds then converted the funds for his own personal use.

To conceal his theft from other UAW officers and the Local 412 members, Edmunds created false bank statements and caused false Department of Labor ("DOL") reports to be filed with the U.S. DOL. Edmunds supplied the fake bank statements to international UAW auditors in an effort to conceal his embezzlement.

Edmunds used portions of the proceeds of his embezzlement to gamble extensively, to purchase firearms, and to purchase various high-end vehicles. For example, between 2018 and 2020, Edmunds used the UAW Local 412 debit card to make over $30,000 in unauthorized withdrawals at the Greektown Casino. While gambling at the Greektown Casino, records indicate that Edmunds had cash buy-ins of over $1 million, and he put over $16 million in play while gambling at the casino. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Former Pharmaceutical Executive Accused Of Stealing Trade Secrets And Giving Them To Boyfriend Who Was CEO Of Competitor - July 11, 2022

In a lawsuit filed in a federal court in Pennsylvania, the drug giant Teva is alleging that its former Chief Of Regulatory Affairs for its American generics business passed trade secrets to her boyfriend, who happened to be the CEO of generics industry rival Apotex.

But it's far more than two lovers engaging in pillow talk about generic pills, Teva claims. The lawsuit alleges that, over a period of about two years ending in 2016, Teva employee Barinder Sandhu copied company files onto flash drives and passed them to Apotex CEO Jeremy Desai. Sandhu was fired in October 2016>

Teva hired Sandhu in 2012 and promoted her to the Regulatory Affairs position in the spring of 2014, handing her a salary of $193,000 plus a potential annual bonus of 30% of that haul. A few months later, Desai was named CEO of Apotex. The two were already romantically involved and living together in Pennsylvania.

An internal investigation revealed that Sandhu created a folder on her Teva-issued computer called "My Drive," which synced to a personal cloud account—and that she uploaded 900 Teva files to that folder, including trade secrets and other confidential information. She also copied files to as many as 10 USB drives, Teva alleges. The use of cloud backup and external drives violated the confidentiality agreement she signed upon accepting employment with the company.

Teva learned of Sandhu's actions from a former Apotex employee, who reported that Apotex used the information she shared with Desai to compete against Teva. The documents included confidential communications with the FDA about an unnamed drug Teva was developing, which Apotex reportedly used to "speed the regulatory approval of its competing product," according to the lawsuit. (Source)

Former Employee Of Construction Firm Quits Company And Downloads A Trove Of Confidential Information - July 22, 2022

Williams Company is a construction company with a portfolio of major projects at SeaWorld Orlando and Legoland Florida as well as building Orlando's Boone High School, Stetson University Rinker Welcome Center and numerous other commercial buildings.

On his way out the door, Paul Comazzi, the ex-employee obtained documents such as the company's bank account statements and tax returns as well as 401(k) information containing employees' names, Social Security numbers, birth dates and their compensation.

Comazzi, first hired as a Project Manager in 2017, rose through the ranks and was promoted to Construction Technology Manager.

On Jan. 28, 2022 Comazzi resigned. He told the company it was for unforeseen personal issues. Comazzi told colleagues the reason for his resignation was that he wanted to wake up at noon and play video games all day.

Two months later, the company learned about the data breach and that Comazzi shared the information with nonexecutive employees. Comazzi's former co-workers warned the company what happened. Comazzi had misused a colleague's login to access confidential and proprietary business information. Comazzi also gave the information to other third parties, none of whom had any right, entitlement to or access to this information.

The lawsuit describes a contentious relationship between Comazzi and the company's leaders before he quit. The company alleged in the lawsuit that Comazzi was sharing the stolen information to further fuel his conspiracy theory and flame false narratives about the Company and its senior management in an effort to create chaos and discord at the company. (Source)

Former McDonald's Restaurant Employee Arrested For Identity Theft Of 70+ Customers - July 27, 202

Police are investigating complaints of a crimes committed by a drive thru window employee at a McDonald's Restauran. It is alleged that Dayshia Nicole Hardy photographed credit and debit cards used at the window to pay for food. It is further alleged that Hardy sold that information.

So far there have been 29 people confirmed as possible victims of identity theft because of an Hardy's actions. There are reports suggestubg that there could be as many as 70 or 80 individuals who have had their personal information compromised by Hardy. (Source)

PHARMACEUTICAL COMPANINES / PHARMICIES / HOSPITALS / HEALTHCARE CENTERS / DOCTORS OFFICE & STAFF

No Incidents To Report

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

U.S. Attorney Announces Charges In 4 Separate Insider Trading Cases Against 9 Individuals, Including Former U.S. Congressman, Former FBI Agent Trainee, Tech Company Executives, And Former Investment Banker - July 27, 2022

Former U.S. Congressman Charged with Insider Trading Based on Inside Information Obtained from Consulting Work

Former FBI Agent Trainee and Friend Charged with Insider Trading Based on Inside Information Stolen from the Trainee's former Girlfriend

Network of Individuals Charged with Insider Trading based on Inside Information obtained from the Former Chief Information Security Officer of Telecommunications Company

New York based Investment Banker Charged with Insider Trading for Using Stolen Information about Potential Investments to Tip Trading Friend

These cases involve trading based on confidential information misappropriated from entities and individuals in a variety of industries and reflect the U.S. Attorney's Office for the Southern District of New York's broad investigative reach and continued resolve to root out corruption in our financial markets. The defendants in these cases made between hundreds of thousands and millions of dollars from illegal securities trading based on material, non-public information that was stolen from numerous sources. (Source)

Former Chief Financial Officer Pleads Guilty To Embezzling $16 Million+ Over 9 Years To Finance Personal Lifestyle & Business Ventures - July 27, 2022

For nearly a decade, Frank Okunak was the Chief Financial Officer and later Cief Operating Officer of a leading global public relations (PR) firm.

Okunak embezzled over $16 million from the PR Firm and, ultimately, the shareholders of the PR Firm's publicly traded parent corporation.

Okunak used the embezzled funds to finance his personal lifestyle and his own private business ventures. Okunak concealed and facilitated his theft by preparing and causing others to prepare materially false accounting books and records, including invoices and payment records that falsely described expenditures as having been undertaken for the benefit of the PR Firm, when funds were actually used for Okunak s personal benefit or for the benefit of his personal business associates. (Source)

Former Financial Controller Admits To Embezzling $2.37 Million From His Employer For 6 Years - July 14, 2022

From 2014 through December 2020, Gerard Beauzile abused his position as controller of a New York-based company to embezzle funds by issuing fraudulent company checks to himself and then depositing those checks into his bank account for his own personal benefit. B

Beauzile issued approximately 140 company checks to himself with a total value of $2.37 million. Beauzile concealed the theft from the company by falsely entering the fraudulent checks into the company's accounting system under various company vendor names as the payees, causing the accounting system to falsely reflect that the checks were made payable to company vendors instead of to Beauzile. He also falsified vendor invoices to correspond to the entries made in the accounting system, and company bank statements by removing and altering opening, running, and closing balances, check payment entries, summary check listings, and inter-account transfers. (Source)

Former Chief Operating Officer Charged With $2.1 Million+ Of Wire Fraud To Pay For Personal Expenses - July 29, 202

Between January 2012 and January 2019, while employed as the Chief Operating Officer for Simple Helix, LLC in Huntsville, Ray Shickles devised and executed a scheme to fraudulently obtain money from Simple Helix.

As part of the scheme, Shickles gained access to PayPal accounts of Simple Helix and made multiple unauthorized charges, withdrawals, and transfers from those accounts to pay for personal expenses. Shickles also created a fraudulent email account for Simple Helix and caused funds intended for Simple Helix to be deposited into personal accounts of Shickles. Shickles took steps to conceal his fraudulent activities by causing a computer-generated report of financial activities of Simple Helix to exclude his fraudulent transactions. The fraudulent transfers caused by Shickles resulted in a loss to Simple Helix of over $2.1 million dollars.(Source)

Former Accounts Payable Processor Sentenced To Prison For $1.7 Million+ Wire Fraud Scheme - July 11, 2022

From at least October 2019 through May 21, 2021, Theresea Walker was employed as an accounts payable processor with a technology company, defense contractor, and information technology services provider headquartered in Melbourne, Florida.

In this role, Walker's responsibilities included accessing her employer's payment software systems for the purpose of entering vendor and supplier invoices and scheduling those invoices for payment. Walker's employer conducted an audit of accounts serviced by Walker and the audit revealed that Walker had made false entries into the employer's accounts payable system to conduct nine wire transactions through which Walker caused the transfer of funds from the employer's bank account to accounts controlled by Walker.

As part of her scheme, Walker also edited the payment terms and accounts of actual existing vendors with the employer, so that new invoices entered under that vendor name would be paid directly to the accounts designated by Walker. During the course of the scheme, in an attempt to hide her fraudulent activity, Walker created multiple fictitious invoices and fraudulent credit memos. Walker caused a total loss of $1,757,082.73 to the employer, which also represents the proceeds received by her from her scheme. (Source)

Former Employee Sentenced To 65 Years In Prison For Stealing $288,000+ From Employer / Previously Stole $106,000 From Another Company - June 10, 2022

Leslie Garcia had worked for a company in Sugar Land, Texas, where she was one of the highest-paid employees. But that didn't stop her from stealing $288,846.92 over the course of 22 months. She deposited 29 unauthorized checks into a new bank account before her ruse was discovered. And this wasn't her first theft of this kind.

In 2008, Garcia received an eight-year prison sentence for stealing $106,000 from a company in Rosenberg, Texas. Back then, she also utilized unauthorized checks to give herself a pay raise and two loans before the owners realized what she was doing. She got out from parole only 47 days when she began stealing from the company in Sugar Land. The owners stated they were not aware of Garcia's previous crime. At trial, she tried to deny getting fired from the owners in addition to denying her stealing funds and the existence of her fraudulent bank account. (Source)

Former Director Of Accounting & Human Resources Pleads Guilty To Embezzling $630,000+ For Jewelry, Beauty Treatments, Travel, Pets, Clothing, Cars - July 1, 2022

In October 2019, Susana Rivera was hired as the Director of Accounting and Human Resources for a family owned kitchen design and remodeling business.

Starting in November 2019, Rivera made hundreds of unauthorized charges in a total amount exceeding $175,000 to the victim company's credit cards for personal expenses, including jewelry, beauty treatments, laser treatments, travel, pets, cosmetic surgery, clothing and cars, including a partial payment on a $100,000 Corvette.

Rivera also caused the victim company's payroll company to make unauthorized payments in a net amount of more than $370,000 to a fake vendor that Rivera created to receive the money. Rivera also caused unauthorized transfers from the victim company's bank account in an amount exceeding $2,900 to pay her personal utility bills. To get restrictions on the use of the victim company's credit cards removed, Rivera posed as an owner of the victim company in telephone calls with the company's credit card company. Rivera also sent the credit card company photographs of the owner's driver's license to cause credit card company personnel to believe she was the owner. (Source)

Former Office Manager Sentenced To Prison For Stealing $587,000+ From Her Employer To Make Amazon Purchases & Buy A Boat - July 7, 2022

Jessica Pechtel was the Office Manager for a company in Somersworth, New Hampshire. In that role, she had full access to the company's finances, including its accounting records, bank accounts, and company credit card.

Pechtel used her access to the company's finances to make unauthorized purchases and transfers of funds to accounts that she controlled. Pechtel engaged in a multifaceted scheme for at least a year and a half to steal the funds. First, she transferred funds from the company's bank accounts to her own accounts. Additionally, she used the company's credit card to make unauthorized purchases from retailers such as Amazon or make payments via the online payment transfer system Venmo. Pechtel also drafted 17 unauthorized checks payable to herself that were drawn on the company's bank account. And lastly, she stole almost $44,000 in COVID-19 relief funds that were intended for the company.

Pechtel also took steps to conceal her embezzlement. She created and controlled a PayPal account in the name of one of her coworkers to transfer funds. She manipulated the company's accounting records to make her fraudulent transfers appear like payments to legitimate vendors. (Source)

Overall, Pechtel fraudulently obtained at least $587,219 from her employer. Those funds were used for various personal expenses such as Amazon purchases and the purchase of a boat. (Source)

Former Employee Sentenced To Prison Stealing $213,000 + From Employer - July 13, 2022

Rodney Roussell began working for his company through a work re-entry program for persons with criminal records. The company maintained a business account with JPMorgan Chase Bank.

Roussell did not have access to company Chase Bank account, and was not authorized to make payments of any kind using funds in the account. Beginning in or about April 2018, and continuing until in or about June 2018, Roussell utilized Chase Bank's web portal and mobile banking app to transfer money from the company's account to accounts held by Roussell.

Roussell illegally obtained $213,372.05 from the company's Chase Bank account. (Source)

Former Bookkeeper Sentenced To Prison For Defrauding 3 Small Businesses Of $156,000 For Personal Expenses - July 12, 2022

Alicia Merritt admitted to stealing $156,734.76 from three small businesses that employed her as a part-time bookkeeper, and she was sentenced to prison and ordered to pay restitution to the victims.

Merritt's theft from Willow Oaks Landscape was first discovered by the company's owner in Feb. 2020. Merritt worked as the bookkeeper for the family-owned business for a decade and the owner trusted her completely, delegating to her payroll, vendor payments, reimbursements and giving her credit card access. When the business began to lose money, the owner assumed there must be other causes and didn't suspect Merritt. However, from March 2019 until Feb. 2020, Merritt wrote checks to vendors, to herself for reimbursements that did not exist and cut payroll checks for former employees and cashed them for herself in the amount of $108,068.45. In addition, within this same time frame, Merritt admitted to charging $5,382.90 on the company credit card for personal expenses.

Merritt was also employed part-time managing business finances for two local Eatonton businesses, The Meat Shed and Vape on the Lake. Merritt was tasked with handling business tax payments to the Georgia Department of Revenue and IRS for the businesses. In early 2019, Merritt constructed a scheme, convincing the owner that she could better manage his tax payments if he wrote her checks for the amount owed and she, in turn, would pay the tax to the relevant revenue agency. In late 2019, Merritt's demands escalated, insisting the owner write multiple large payments to resolve alleged tax payment deadlines, keeping the money for herself and not paying the taxes owed. In all, Merritt stole at least $33,209.31 from these businesses. (Source)

Former Director Of Utilities Sentenced To Prison For Accepting Bribes Of $30,000+ - July 16, 2022

From 2012 to 2018, Barry Edwards and an unnamed individual identified in court documents as the Contractor, devised a bribery and kickback scheme involving the Catawba County Government.

Edwards admitted in court, as Director of Utilities and Engineering, Edwards had the authority to review and award contracts on behalf of the County government to private businesses, for engineering and consulting activities related to the County's landfill, and solid waste and natural gas projects, among others.

Edwards admitted to awarding contracts to three businesses associated with the Contractor, all while receiving gifts and other things of value that influenced his decisions, such as expensive meals, tickets to sporting events, and wine-tasting tours, totaling more than $30,000. (Source)

Former Purchasing Agent Sentenced To Prison For Embezzling $400,000+ To Purchase All Terrain Vehicles, Tractor, Firearms, Ammunition & Camping Equipment - July 20, 2022

Kyle Hollman was employed as a Purchasing Agent for ProLift Toyota Material Handling, and his job was to procure equipment for Aleris Rolled Products.

Hollman used funds belonging to his employer and Aleris to fraudulently purchase hundreds of items for his own personal use, including, two all-terrain vehicles (ATVs), a tractor, firearms, ammunition, firearm accessories, tools, tactical gear, and camping equipment. Hollman made around 847 unauthorized purchases, totaling $346,608.65, from Feb. 20, 2018, to Nov. 12, 2020.

Hollman perpetrated his fraud scheme by billing Aleris for products that ProLift never purchased, providing inflated invoices, altering receipts, and using company credit cards for unauthorized purchases. Hollman defrauded Aleris of more than $422,693.40. (Source)

Former Chief Financial Officer Admits Defrauding Employer And Lender Of $700,000 - July 19, 20222

Margaret Boisture functioned as the Chief Financial Employee of ZoneFlow Reactor Technologies, a pre-revenue company in the business of developing and commercializing a new technology that improves the efficiency of the production of hydrogen. PayPal marketed and serviced commercial loans from WebBank, a third-party lender.

Between approximately October 2016 and February 2020, Boisture defrauded ZoneFlow, PayPal and WebBank by diverting ZoneFlow money to herself; taking unauthorized loans that caused ZoneFlow to pay additional interest expense; and making misrepresentations to PayPal and WebBank to induce them to make unauthorized loans to ZoneFlow that expanded the pool of money from which Boisture could take.

In total, Boisture's criminal conduct caused losses of $632,159.78 to ZoneFlow and $78,066.76 to PayPal and WebBank. (Source)

Former Office Manager Sentenced To Prison For Embezzling $100,000+ From Employer Over 5 Years - July 22, 2022

From approximately March 2009 to November 2017, LaDonna Livers worked as the Office Manager for an Evansville business. As the office manager, she oversaw and conducted all financial operations for the business.

Livers used her position to illegally enrich herself by embezzling funds from her employer's bank accounts. Over the course of approximately five years, Livers stole $109,743.73 from her employer by making unauthorized transfers from the employer's bank accounts to her own bank and credit card accounts. (Source)

SHELL COMPANIES / FAKE INVOICE BILLING SCHEMES

No Incidents To Report

NETWORK / IT SABOTAGE

No Incidents To Report

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

THEFT OF COMPANY PROPERTY

Former Philadelphia Water Department Employee Sentenced To Prison For Stealing $150,000+ Of Assets - July 6, 2022

Thomas Staszak is a former employee of the City of Philadelphia Water Department (PWD).

On multiple occasions from approximately April 2017 through at least November 2018, Staszak accessed the PWD's computerized inventory control system without authorization, using log-in credentials associated with PWD employees under his supervision at a PWD storeroom.

Staszak is then charged with creating false entries in PWD's electronic records to provide justifications for removing maintenance materials, for example bulk wire, from the storeroom. Staszak then physically took the materials from PWD's inventory, transported them to local scrap yards, sold the materials, and kept the proceeds. Staszak stole items valued at approximately in excess of $150,000 before he was caught. (Source)

EMPLOYEE DRUG RELATED INCIDENTS

Former Elizabeth Borough Police Chief Charged with Stealing Heroin From Evidence For Personal Use - July 19, 2022

From June 2017 until December 2018, Timothy Butler, was the former Chief of Police.

He stole evidence, bricks of heroin with a value of over $1,000 from the Elizabeth Borough Police Department evidence locker for his own personal use. (Source)

Former Hospital Nurse Pleads Guilty To Fraudulently Obtaining Controlled Substances From 3 Health Care Facilities - July 27, 2022

Angelica Franklin was a registered nurse with the Virginia Department of Health Professions Board of Nursing. On August 16, 2021 she began working in the Emergency Department at Sentara Martha Jefferson Hospital (SMJH) in Charlottesville.

Franklin admitted today that in September 2021, she knowingly and intentionally entered fraudulent verbal orders for fentanyl and hydromorphone into the SMJH electronic medical records system on behalf of physicians who did not issue the verbal orders. Franklin then obtained the fentanyl and hydromorphone from the SMJH automated dispensing cabinet but did not administer the controlled substances to patients.

In addition, Franklin admitted to unlawfully obtaining controlled substances fentanyl, hydromorphone, oxycodone, and alprazolam while working as a nurse at three Richmond-area health care facilities: Stony Point Surgery Center, Vibra Hospital, and The Laurels of Willow Creek.

In total, across all facilities, Franklin unlawfully obtained approximately 4,450 mcg of fentanyl, 80 mg of hydromorphone, 3,600 mg of oxycodone, and 14 mg of alprazolam. (Source)

EMPLOYEE MASS LAYOFF INCIDENTS

No Incidents To Report

WORKPLACE VIOLENCE

Spectrum Cable Company Ordered To Pay $7 BILLION+ In Damages For Employee Who Murdered Customer Because Of Systemic Spectrums Failures In The Pre-employee Screening, Hiring & Supervision Practices - July 29, 2022

The Spectrum cable company has been ordered to pay over $7 billion in damages to the family of 83 -year old Texas grandmother (Betty Thomas) who was brutally stabbed to death in her home by a Spectrum employee in 2019.

Roy James Holden, an installer for Spectrum, owned by Charter Communications, had performed work at Thomas' home in Irving in December 2019, police said at the time.

Holden returned the next day in uniform and using the company's van while he was off, posing as if he was on the job, and killed her, then used her cards for a shopping spree after her murder.

The jury previosly found Charter Communications negligent and grossly negligent in Thomas' death.

The jury awarded a verdict of $375 million in compensatory damages and said the company was responsible for paying 90% of it after the trial revealed "systemic failures" in the company's pre-employee screening, hiring and supervision practices.

Recently the verdict for punitive damages was announced, bringing the total to $7.37 billion. (Source)

Amazon Employee Arrested / Was Planning Mass Shooting At Amazon Facility – July 3, 2022

Rodolfo Aceves, a San Antonio man, was arrested after people at his job reported him for allegedly saying he was planning a mass shooting.

Aceves, 19, was apprehended after San Antonio Police responded to an Amazon Delivery Station, where the teenager worked, at around 10:30 a.m. on June 27. Officers talked to several people who reported hearing Aceves say he was planning a mass shooting at the facility.

Police detectives were then notified and they "acquired credible information" to believe the comments were taken as a "legitimate potential mass shooting threat."

Detectives also seized an AR-15 in his possession. (Source)

EMPLOYEE INVOLVED IN TERRORISM

No Incidents To Report

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

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEES WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

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

Former Credit Union Employee Pleads Guilty To Unauthorized Access To Computer System After Termination & Sabotage Of 20+GB's Of Data (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)

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)

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)

WORKPLACE VIOLENCE

Spectrum Cable Company Ordered To Pay $7 BILLION+ In Damages For Employee Who Murdered Customer Because Of Systemic Spectrums Failures In The Pre-employee Screening, Hiring & Supervision Practices - July 29, 2022

The Spectrum cable company has been ordered to pay over $7 billion in damages to the family of 83 -year old Texas grandmother (Betty Thomas) who was brutally stabbed to death in her home by a Spectrum employee in 2019.

Roy James Holden, an installer for Spectrum, owned by Charter Communications, had performed work at Thomas' home in Irving in December 2019, police said at the time.

Holden returned the next day in uniform and using the company's van while he was off, posing as if he was on the job, and killed her, then used her cards for a shopping spree after her murder.

The jury previosly found Charter Communications negligent and grossly negligent in Thomas' death.

The jury awarded a verdict of $375 million in compensatory damages and said the company was responsible for paying 90% of it after the trial revealed "systemic failures" in the company's pre-employee screening, hiring and supervision practices.

Recently the verdict for punitive damages was announced, bringing the total to $7.37 billion. (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

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 (**3,900+ Incidents**).

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

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

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

(**500+ Incidents**)

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 Linked 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.

Insider Threat Program Development – Management Training Course / Classroom Based: Sterling, Virginia, August 22 & 23, 2022

In addition to the main instructor, this class will also have 2 additional instructors who are the former ITP Managers for CIA and NSA, and have extensive knowledge of ITP Development - Management in the U.S Government, Department of Defense, Intelligence Community and the private sector.

Complete Details / Registration / Cost: $1,495 With Money Back Guarantee
https://www.eventbrite.com/e/insider-threat-program-development-management-training-course-tickets-381120671187

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