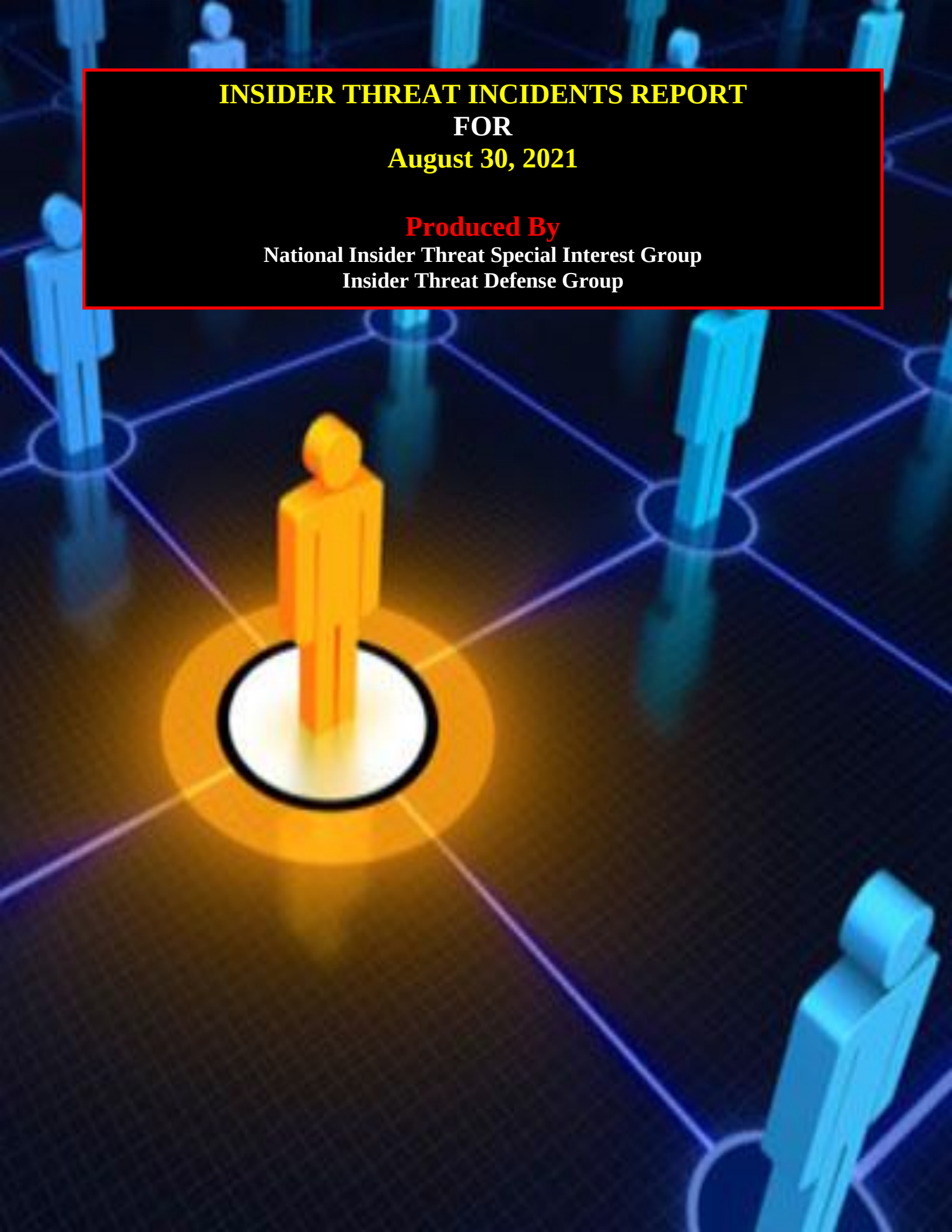

INSIDER THREAT INCIDENTS REPORT
FOR
August 30, 2021

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 **2,900** 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 11 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
- ☐ Data, Computer & Network Sabotage
- ☐ 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 AUGUST 2021

U.S. GOVERNMENT

Former U.S. Postal Service Employee Admits Stealing Credit Cards From Mail Resulting In $100,000 Loses To Victims - August 24, 2021
https://www.justice.gov/usao-nj/pr/former-essex-county-postal-employee-admits-stealing-credit-cards-mail-access-device-fraud

DEA Agent Sentenced To Prison In Corruption Case / 3 Other Agents Convicted - August 12, 2021
https://www.foxnews.com/us/dea-agent-sentenced-corruption-case

Former USDA Official Sentenced To Prison For Bribery For Preferential Treatment In The Award Of $19 Million Of Security Contracts - August 10, 2021
https://www.justice.gov/usao-dc/pr/former-usda-official-sentenced-bribery-caseformer-usda-official-sentenced-bribery

Former U.S. Postal Service Carrier Sentenced To Prison For Dumping 5,800+ Pieces Of Mail In Woods - August 4, 2021
https://www.justice.gov/usao-ndny/pr/former-postal-carrier-sentenced-discarding-mail-woods

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Army National Guardsman & DoD Subcontractors Charged Conspiring To Steal And Sell Military Gear / Uniforms - August 19, 2021
https://www.justice.gov/usao-sdil/pr/missouri-army-national-guardsman-and-department-defense-subcontractors-indicted

Veterans Affairs Employee (Purchasing Agent) Pleads Guilty To Theft Of $1.9 Million Of VA Equipment - Which He Then Sold - August 16, 2021
https://www.justice.gov/usao-ndga/pr/veterans-affairs-employee-pleads-guilty-theft-medical-equipment

3 Former Fort Bragg Employees Accused Of Receiving $ 1 Million+ In Bribes For Contracts - August 13, 201
https://www.justice.gov/usao-ednc/pr/former-ft-bragg-employees-accused-receiving-bribes

Former NGA Intelligence Analyst Sentenced To Prison For Disclosing Classified Information to Reporter - July 27, 2021
https://www.justice.gov/opa/pr/former-intelligence-analyst-sentenced-45-months-prison-disclosing-classified-information

Former U.S. Army Employee Pleads Guilty To Kickback Scheme To Steer $3 Million+ Of U.S. Government Contracts - July 21, 2021
https://www.justice.gov/opa/pr/former-us-army-employee-pleads-guilty-kickback-scheme-steer-us-government-contracts

LAW ENFORCEMENT

Former Police Officer Pleads Guilty For Stealing Narcotics From Evidence Locker, Overdosing & Then Wrecking Police Car - August 24, 2021
https://www.justice.gov/usao-or/pr/former-klamath-falls-police-officer-pleads-guilty-stealing-methamphetamine-and-fentanyl

Former Sheriff Convicted Of Public Corruption Charges Involving Mail Fraud, Money Laundering Over 22 Years - August 24, 2021
https://www.justice.gov/usao-edva/pr/former-norfolk-sheriff-convicted-public-corruption-charges

6 Maryland Law Enforcement Officers Facing Federal Charges Related To Schemes to Defraud Financial Institutions And Insurance Companies For Personal Profit - August 18, 2021
https://www.justice.gov/usao-md/pr/six-maryland-law-enforcement-officers-facing-federal-indictment-charges-related-schemes

Former Detroit Police Department Officer For 19 Years Sentenced To Prison For Accepting $15,000 Bribe - August 6, 2021
https://www.justice.gov/usao-edmi/pr/former-detroit-police-department-officer-sentenced-18-months-bribery

Former Boston Police Auto Repair Technician Pleads Guilty To 3 Year $260,000 Wire Fraud Scheme Fraud - July 30, 2021
https://www.justice.gov/usao-ma/pr/former-boston-police-auto-repair-technician-agrees-plead-guilty-wire-fraud-charges

STATE / CITY GOVERNMENTS / SCHOOL SYSTEMS

Former Senior Building Inspector & Building Inspection Commission President Charged With Building Permit Fraud / Asking For Charitable Contributions - August 19. 2021
https://www.justice.gov/usao-ndca/pr/former-san-francisco-senior-building-inspector-and-former-san-francisco-building

Former Louisiana City Employee Sentenced To Prison For $400,000+ Credit Card Fraud & Identity Theft - August 13, 2021
https://www.justice.gov/usao-wdla/pr/former-city-shreveport-employee-sentenced-conspiracy-and-aggravated-identity-theft

Former North Carolina Social Services Employee Sentenced To Prison For Theft Of $200,000+ Of State Government Funds - August 13, 2021
https://www.justice.gov/usao-ednc/pr/former-social-services-employee-harnett-county-sentenced-theft-government-funds

Former School Custodian Who Had Been Terminated Was Having Homicidal Thoughts Is Accused Of Planning Mass Casualty Event At School - August 5, 2021
https://amp.cnn.com/cnn/2021/08/05/us/oregon-school-custodian-arrest-mass-casualty-event/index.html

Georgia Teacher Who Was Put On Administrative Leave, Returns To School The Next Day & Starts Fire, Shooting Gun Inside School - August 9, 2021
https://www.foxnews.com/us/georgia-teacher-faces-arson-charge-middle-school

Former High School Assistant Principal Sentenced To Prison For Scamming School System Out Of More Than $300,000 With Fake Invoices - August 11, 2021
https://www.justice.gov/usao-mdal/pr/former-montgomery-high-school-assistant-principal-sentenced-scamming-school-system-out

9 Employees Of The Philadelphia Bridges And Buildings Department And Vendors Charged In $870,00 Bribery And Fraud Procurement Scheme - August 11, 2021
https://www.justice.gov/usao-edpa/pr/nine-septa-maintenance-managers-and-vendors-charged-bribery-and-fraud-connection

Housing Authority Director And 4 Others Charged With $5.8 Million Wire / Bank Fraud Scheme For Personal Use & Casinos - July 21, 2021
https://www.southbendtribune.com/story/news/2021/07/20/former-director-south-bend-housing-authority-charged-fraud/8033949002/

Trash Company Executive Agrees Plead Guilty To Bribing San Francisco Public Works Official For Contracts - July 28, 2021
https://www.justice.gov/usao-ndca/pr/trash-company-executive-agrees-plead-guilty-conspiracy-and-cooperate-federal

Former Township Clerk Sentenced To Prison For $650,000+ Wire Fraud Scheme Over 8 Years For Personal Use - July 27, 2021
https://www.justice.gov/usao-mn/pr/former-vermillion-township-clerk-sentenced-prison-650000-wire-fraud-scheme

BANKING / FINANCIAL INSTITUTIONS

Former Bank Officer Sentenced To Prison For $2.3 Million Embezzlement Scheme For Personal Benefit Over 5 Years - April 4, 2020
https://www.justice.gov/usao-wdok/pr/former-metro-employee-trust-bank-sentenced-serve-30-months-federal-prison-23-million

EMBEZZLEMENT / FINANCIAL THEFT / BRIBERY / KICKBACKS

Former Employee Sentenced To Prison For Defrauding His Former Employer Of $4 Million+ To Buy Condo, RV, Boat, Cars, Trucks - August 26, 2021
https://www.justice.gov/usao-wdnc/pr/denver-nc-man-sentenced-four-and-half-years-prison-defrauding-his-former-employer-more

Former Office Manager Pleads Guilty To $330,000+ Of Wire & Credit Card Fraud - August 25, 2021
https://www.justice.gov/usao-edla/pr/laplace-woman-pleads-guilty-wire-fraud

Former Employee & 4 Conspirators Involved In $2+ Million Fraud Scheme - August 25, 2021
https://www.justice.gov/usao-md/pr/conspirator-scheme-defraud-maryland-company-more-2-million-sentenced-three-years-federal

Former Air Conditioning Contractor Paid $93,000 In Bribes To Obtain Permits From City Inspector - August 11, 2021
https://www.wdsu.com/article/former-new-orleans-building-inspector-pleads-guilty-to-accepting-bribes/37284547

Former Walmart Employee Pleads Guilty To Stealing $123,00+ Worth Of Gift Cards - August 24, 2021
https://www.justice.gov/usao-ndwv/pr/ohio-man-admits-wire-fraud-charge

Former Chief Financial Officer Sentenced To Prison For Embezzling $930,000+ From Employer Over 6 Years For Personal Expenses - August 23, 2021
https://www.justice.gov/usao-mn/pr/former-cfo-sentenced-prison-embezzling-more-900000-employer

Former Bookkeeper Sentenced To Prison For $1 Million+ Mail Fraud And Money Laundering Scheme Over 6 Years - August 20, 2021
https://www.justice.gov/usao-co/pr/fort-collins-bookkeeper-sentenced-mail-fraud-and-money-laundering

Former Employee Sentenced To Prison For Stealing $400,000+ Over 4 Years For Personal Use- August 18, 2021
https://www.justice.gov/usao-sdtx/pr/former-employee-sentenced-stealing-over-400000

Former Bookkeeper Sentenced To Prison For Embezzling $1.24 Million Over 9 Years - August 18, 2021
https://www.justice.gov/usao-ndga/pr/former-bookkeeper-sentenced-prison-embezzlement

Former Netflix Software Engineer Pleads Guilty To Insider Trading - He Receives $60,000 In Cash For Tips - August 18, 2021
https://www.justice.gov/usao-wdwa/pr/bellevue-man-pleads-guilty-profiting-inside-information-netflix-securities-trades

Former Ironworkers Treasurer Sentenced To Prison For Stealing $50,000+ Of Union Funds To Pay For Personal Expenses - August 18, 2021
https://www.justice.gov/usao-wdny/pr/former-ironworkers-treasurer-sentenced-stealing-union-funds

Former U.S. Golf Association Employee Charged With Stealing 23,000+ Tickets Worth $3 Million+ And Then Selling Them Over 7 Years
https://www.justice.gov/usao-edpa/pr/former-us-golf-association-employee-charged-embezzling-over-3-million-us-open-tickets

Former Law Firm Office Manager Sentenced To Prison For Embezzling $425,00 From Firm - August 16, 2021
https://www.justice.gov/usao-dc/pr/new-jersey-man-sentenced-41-months-prison-embezzling-money-law-firm

Company Accountant Sentenced To Prison For $140,000 Of Wire Fraud - August 6, 2021
https://www.justice.gov/usao-edla/pr/new-orleans-man-sentenced-wire-fraud

Former Law Firm Employee Sentenced To Prison For Embezzling $320,00 From Firm Over 4 Years - August 5, 2021
https://www.justice.gov/usao-dc/pr/maryland-woman-sentenced-30-months-prison-embezzling-money-law-firm

Former Bed & Breakfast Manager Accused Of Embezzling $500,000+ For Personal Use - August 4, 2021
https://www.justice.gov/usao-sdga/pr/savannah-bb-manager-accused-embezzling-more-half-million-dollars

Trusted Payroll Company Involved In A $100,000 Million+ Fraud Scheme Over 7 Years That Affected Banks, Financing Companies & Other Businesses - August 4, 2021
https://www.justice.gov/usao-ndny/pr/valuewise-ceo-michael-mann-sentenced-144-months-prison-100-million-fraud

Former Employee Pleads Guilty To Engaging In Wire Fraud Conspiracy With Co-Worker To Defraud Former Employers Of $546,000+ For Personal Use - July 28, 201
https://www.justice.gov/usao-nj/pr/connecticut-woman-admits-engaging-conspiracy-defraud-former-employers

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

German Healthcare Worker Swapped Vaccine For Saline - 9,000 Patients Possibly Effected - Worker Was Critical Of Vaccine - August 10, 2021
https://www-businessinsider-com.cdn.ampproject.org/c/s/www.businessinsider.com/9000-people-germany-vaccinations-nurse-swapped-vaccines-for-saline-2021-8?amp

Former Hospital Nurse Charged With Tampering / Removing Pain Medication From Vials And Replacing With Other Liquid - August 25, 2021
https://www.justice.gov/usao-edmi/pr/former-nurse-charged-tampering-consumer-products

Physician Assistant Sentenced To Prison For The Unauthorized Distribution Of Pain Medications At Pain Management Practice - August 26, 2021
https://www.justice.gov/usao-md/pr/physician-assistant-sentenced-three-years-federal-prison-conspiring-distribute-and

Former Hospital Technician Sentenced To Prison For Secretly Recording 58 Undressed Patients / Lawsuits Pending - August 16, 2021
https://triblive.com/local/ex-west-penn-hospital-technician-gets-jail-for-secretly-recording-undressed-patients/

Former Hospital Procurement Director Sentenced To Prison For $427,000 Bribery Conspiracy Involving Contracts - August 12, 2021
https://www.justice.gov/usao-sdfl/pr/former-procurement-director-broward-health-sentenced-42-months-prison-bribery

Former General Manager For Hospital Dining Facility Pleads Guilty To Theft Of $69,000+ From Cash Registers - August 12, 2021
https://www.justice.gov/usao-wdmo/pr/former-manager-fort-leonard-wood-pleads-guilty-theft

Former Billing Manager For Medical Billing Company Charged With $100,00 Fraud Scheme Using Financial Services Company Square - August 11, 2021
https://www.justice.gov/usao-ndwv/pr/hancock-county-woman-indicted-fraud-charges

Former Medical Office Bookkeeper Pleads Guilty To Embezzling $593,000 Over 5 Years - August 10, 2021
https://www.justice.gov/usao-wdpa/pr/former-medical-office-bookkeeper-pleads-embezzling-nearly-593000-and-filing-false-tax

Former Medical Clinic Employee & Accomplices Plead Guilty To Bank Larceny For Theft Of Over $200,000 Using Patient Information Stolen Medical Clinic - August 10, 2021
https://www.justice.gov/usao-edla/pr/new-orleans-woman-pleads-guilty-bank-larceny-theft-over-200000-using-patient

3 Former Hotel Employees Charged For $153,000 Of Wire Fraud Scheme For Checked Out Guests - August 12, 2021
https://www.justice.gov/usao-sc/pr/charleston-hotel-employees-charged-21-count-federal-indictment-wire-fraud

Mercy Health Fires Marketing & Public Affairs Vice President Suspected Of $3 Million Kickback Scheme - August 18, 2021
https://www.fiercehealthcare.com/hospitals/mercyhealth-reportedly-fires-marketing-public-affairs-vp-suspected-3m-kickback-scheme

Pharmacy Employee Admits To $539,000 Medicare Kickback And Bribery Scheme With Accomplices - July 30, 2021
https://www.justice.gov/usao-nj/pr/morris-county-pharmacy-employee-admits-kickback-and-bribery-scheme

Dental Practice Employees Sentenced To Prison For Ghost Employee $3 Million+ Payroll Scheme - August 11, 2021
https://www.justice.gov/usao-ndin/pr/third-defendant-sentenced-fraud-against-fort-wayne-company

Husband Working For Pharmaceutical Company Provides Wife With Insider Trading Information / Wife Made $286,000 - She Is Now Being Charged - August 18, 2021
https://www.justice.gov/usao-ndil/pr/evanston-woman-charged-insider-trading

DATA / COMPUTER / NETWORK MISUSE & SABOTAGE

Leaked Document Says Google Has Fired 80 Employees Between 2018-2020 For Data Misuse - August 4, 2021
https://www.vice.com/en/article/g5gk73/google-fired-dozens-for-data-misuse

Former Hospital Employee Fired For Unauthorized Access To 1,200+ Individuals Personal Health Information - July 8, 2021
https://www.cbc.ca/news/canada/new-brunswick/charlotte-county-hospital-privacy-breach-health-records-employee-fired-1.6094424

Former Hospital Patient Service Representative & Accomplices Stole Identities Of Dying Patients For COVID Scam - July 23, 2021
https://www.msn.com/en-us/news/us/hospital-worker-stole-identities-of-dying-california-patients-in-covid-scam-feds-say/ar-AAMu36W

Former Urgent Care Employee Accused Of Taking Photos Of Patients' Driver's Licenses And Credit Card Information - July 27, 2021
https://www.wtsp.com/article/news/local/tgh-urgent-care-data-breach/67-32d45bd0-c56f-4c11-9f58-eb9c6887ab25

Former French Intelligence Agent Sentenced To Prison For Selling Confidential Information From Law Enforcement Databases On The Darkweb - August 1, 2021
https://www.suspectfile.com/francia-condannato-ex-poliziotto-per-aver-venduto-informazioni-riservate-sul-darkweb/

Former Security Supervisor Pleads Guilty To $119,000+ Bank Fraud Scheme Using the Stolen Identity Information Of Coworkers & Job Applicants From His Company - July 28, 201
https://www.justice.gov/usao-md/pr/former-security-supervisor-pleads-guilty-bank-fraud-scheme-using-stolen-identity

NEGLIGENT HIRING

Jury Returns Verdict Of $1 Billion In Negligent Hiring Case Against Trucking Firms - 1 Killed / Accident Involved 22 Vehicles - August 24, 2021
https://www.news4jax.com/news/local/2021/08/24/1b-verdict-returned-in-nassau-county-crash-that-killed-unf-student/

WORKPLACE VIOLENCE

86 Years Old Janitor At Sugar Mill Kills Boss When He Found Out He Was Going To Be Fired After 31 Years - July 13, 2021
https://www.dailymail.co.uk/news/article-9781747/Easygoing-janitor-86-shot-boss-dead-31-years-working-going-fired.html

SUMMARIES FOR INSIDER THREAT INCIDENTS LISTED ABOVE

The link below provides a summary of all the incidents listed above:
https://www.insiderthreatdefense.us/insider-threat-incident-postings-for-august-2021/

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEES WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

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

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)

Hackers Looking To Pay $1 Million+ For Disgruntled Employees To Deploy Ransomware Within Employers Networks (2021)

Criminal hackers will try almost anything to get inside a profitable enterprise and secure a million-dollar payday from a ransomware infection. Apparently now that includes emailing employees directly and asking them to unleash the malware inside their employer's network in exchange for a percentage of any ransom amount paid by the victim company.

Crane Hassold, director of threat intelligence at Abnormal Security, described what happened after he adopted a fake persona and responded to hackers proposal. It offered to pay him
40% of a million-dollar ransom demand if he agreed to launch their malware inside his employer's network.

Abnormal Security documented how it tied the email back to a young man in Nigeria who acknowledged he was trying to save up money to help fund a new social network he is building called Sociogram. (Source)

Former Human Resources Manager Convicted Of Deleting Over 17,000 Files (All Of Employers Data) While Being Terminated (2021)

In January 2019, Medghyne Calonge was hired by an online provider of professional services. She was to serve as the head of human resources.

On June 28, 2019, Calonge as terminated for failing to meet the minimum requirements of her job after, among other things, she improperly downgraded a colleague's access to a computer system following an argument with the colleague.

While she was being terminated, and just before she was escorted from the building, Calonge was observed by 2 employees of repeatedly hitting the delete key on her desktop computer. Hours later she logged into a system which the company had invested 2 years and over $100,000 to build. During the next 2 days, she deleted over 17,000 job applications and resumes, and left messages with profanities inside the system. She completely destroyed all her employers data. (Source)

Hackers Looking To Pay $1 Million+ For Disgruntled Employees To Deploy Ransomware Within Employers Networks (2021)

Criminal hackers will try almost anything to get inside a profitable enterprise and secure a million-dollar payday from a ransomware infection. Apparently now that includes emailing employees directly and asking them to unleash the malware inside their employer's network in exchange for a percentage of any ransom amount paid by the victim company.

Crane Hassold, director of threat intelligence at Abnormal Security, described what happened after he adopted a fake persona and responded to hackers proposal. It offered to pay him
40% of a million-dollar ransom demand if he agreed to launch their malware inside his employer's network.

Abnormal Security documented how it tied the email back to a young man in Nigeria who acknowledged he was trying to save up money to help fund a new social network he is building called Sociogram. (Source)

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 (**2,900+ 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 U.S. Government, Department Of Defense, Intelligence Community, United States Space Force, Fortune 100 / 500 companies and others; Microsoft Corporation, Walmart, Home Depot, Nike, Tesla Automotive Company, Dell Technologies, Discovery Channel, Symantec Corporation, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines, Universities, Law Enforcement and many more.

The ITDG has provided training and consulting services to over **640+** organizations. (Client Listing)

Over **875+** 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

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