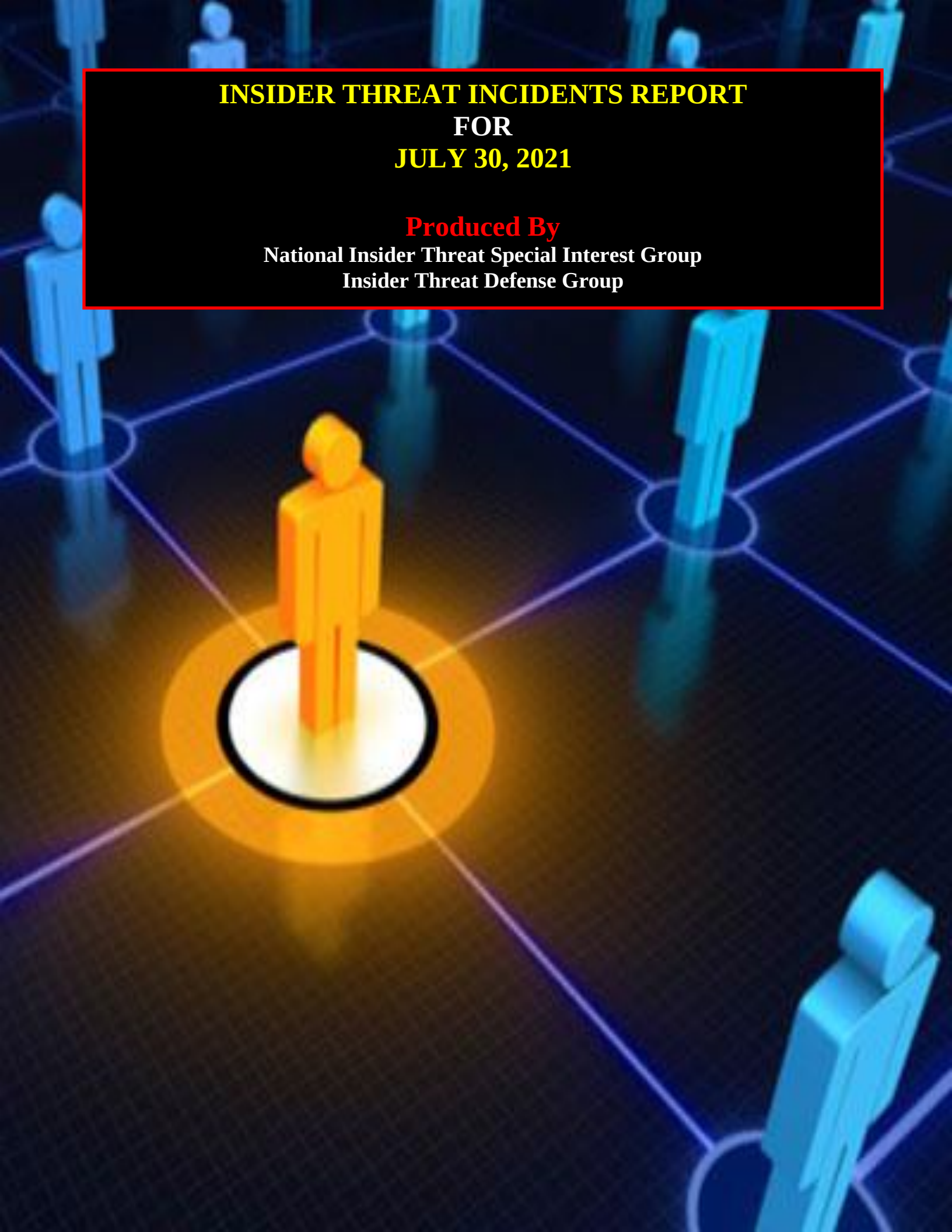


INSIDER THREAT INCIDENTS REPORT
FOR
JULY 30, 2021

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 **2,800** 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 page 5 to 8 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.

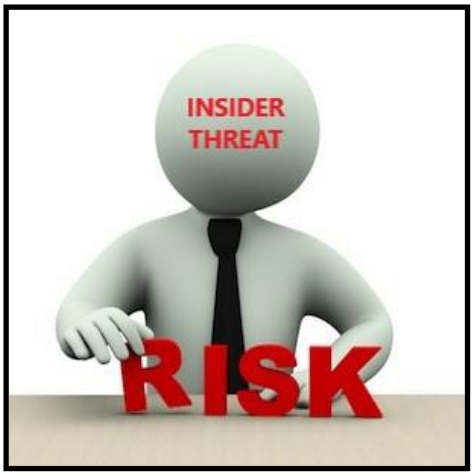
TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

- ☐ 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
- ☐ Information Technology, Computer & Network Or Data 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 JULY 2021

DEPARTMENT OF DEFENSE

Former Executive Assistant Of U.S. Pacific Command In Hawaii Pleads Guilty To Unauthorized Removal / Retention of Classified Information - July 20, 2021

https://www.justice.gov/opa/pr/woman-pleads-guilty-unauthorized-removal-and-retention-classified-material

U.S. Air Force Master Sergeant Sentenced To Prison For Distributing Drugs And Trafficking Firearms - July 13, 2021

https://www.justice.gov/usao-nv/pr/us-air-force-servicemember-sentenced-distributing-drugs-and-trafficking-firearms

Former DoD Official Pleads Guilty To Taking $37,00 In Cash Bribes To Aid Contractor's Request For $6.4 Million From DoD - July 13, 2021

https://www.justice.gov/usao-cdca/pr/former-defense-department-official-pleads-guilty-federal-charges-taking-cash-aid

U.S. GOVERNMENT

Federal Jury Convicts Former IRS IT Specialist Of $58,000+ Fraud For Personal Benefit - July 19, 2021

https://www.justice.gov/usao-edva/pr/jury-convicts-former-irs-employee-fraud

U.S. Postal Worker Arrested For Stealing Blank Postal Money Orders Worth Over $3 Million, Stolen Unemployment Benefits Cards & Over $42,000 In Cash - July 13, 2021

https://www.justice.gov/usao-edny/pr/united-states-postal-worker-arrested-stealing-postal-money-orders

NASA Senior Executive Sentenced To Prison For Covid-19 Loan Fraud To Pay Credit Card Bills - July 17, 2021

https://www.washingtonpost.com/local/legal-issues/tezna-ppp-fraud-conviction/2021/07/16/39ceeb2c-e57b-11eb-a41e-c8442c213fa8_story.html

STATE / CITY GOVERNMENTS / SCHOOL SYSTEMS

Former Parent Teacher Association President Charged For Stealing $5,000+ And Fraud (PTA No Longer Active) - July 12, 2021

https://www.wsmv.com/news/davidson_county/former-pta-president-indicted-on-fraud-theft-charges/article_b3f932e0-e32d-11eb-9092-1bc3afcf9a01.html

County Magistrate Sentenced To Prison For $1 Million Crop Insurance Fraud Scheme Over 7 Years Involving Co- Conspirators - July 15, 2021

https://www.justice.gov/usao-edky/pr/fleming-county-magistrate-sentenced-66-months-crop-insurance-fraud-and-tax-fraud

Former Public Schools Principal Charged In Scheme To Fraudulently Obtain $200,000 In Overtime Pay Over 7 Years - July 14, 2021

https://www.justice.gov/usao-ndil/pr/former-chicago-public-schools-principal-charged-scheme-fraudulently-obtain-overtime-pay

Manager of Water Plant Pleads Guilty Theft Of Funds For Personal Use & Relatives - July 14, 2021
https://www.justice.gov/usao-wdla/pr/manager-water-system-red-river-parish-pleads-guilty-fraud-charge

Former Supervisor For Virginia Department Of Taxation Charged With Embezzling $1.3 Million Of Taxpayer Funds - June 24, 2021
http://www.yourgv.com/news/court/halifax-county-man-indicted-in-tax-fraud-investigation/article_95817654-d524-11eb-9711-bb31d1291674.html

BANKING / FINANCIAL INSTITUTIONS

Bank CEO Convicted Of Corruptly Soliciting A Presidential Administration Position In Exchange For Approving $16 Million In Loans - July 13, 2021
https://www.justice.gov/usao-sdny/pr/bank-ceo-stephen-m-calk-convicted-corruptly-soliciting-presidential-administration

LABOR UNIONS

Former Police Dept. Officer / Union Treasurer Pleads Guilty To Stealing $50,00 Of Union Funds For Personal Expenses - July 20, 2021
https://www.justice.gov/usao-ma/pr/former-new-bedford-police-union-treasurer-agrees-plead-guilty-stealing-union-funds

Former Labor Union President Given Probation For Embezzling $20,000 Of Union Funds - July 12, 2021
https://www.justice.gov/usao-ndok/pr/former-labor-union-president-sentenced-embezzling-union-funds

Former Union President Sentenced To Prison For Embezzling $190,000+ Of Union Funds Over 5 Years, Then Doubling Dues To Continue Fraud
https://www.justice.gov/usao-cdca/pr/former-union-president-sentenced-over-2-years-prison-embezzling-union-funds-then

President Of Union For International Association Of EMT's Pleads Guilty To Embezzling $94,000+Over 6 Years - July 22, 2021
https://www.justice.gov/usao-wdny/pr/local-394-union-leader-pleads-guilty-embezzlement

TRADE SECRET THEFT

Former Genentech Biotechnology Principal Scientist And Her Husband Convicted Of Theft Of Trade Secrets And For Sharing With Taiwanese Biotech Startup & Competitors - July 7, 2021
https://www.justice.gov/usao-ndca/pr/former-genentech-principal-scientist-and-her-husband-convicted-crimes-related-pilfering

Former CEO & COO Of JHL Biotech (Tiawan) Charged With Conspiracy To Steal Trade Secrets From U.S Competitor (Employees From Both Companies Involved) - July 7, 2021
https://www.justice.gov/usao-ndca/pr/former-ceo-and-coo-jhl-biotech-charged-conspiracy-steal-trade-secrets-and-commit-wire

Former Corning Employee Accused Of Theft Of Trade Secrets To Help Start New Business In China - July 7, 2021
https://www.weny.com/story/44259726/former-corning-inc-employee-accused-of-espionage

Former General Manager Of Trailer Sales / Repair Business Steals Trade Secrets Valued At $350,000 To Open Competing Business - July 19, 2021
https://www.jdsupra.com/legalnews/tennessee-federal-court-enjoins-misuse-2299155/

EMBEZZLEMENT / FINANCIAL THEFT

Former Office Administrator Facing Charges Of $700,000+ For Wire Fraud Of Employer To Use For Personal Expenses, Shopping & Dining - July 9, 2021
https://www.justice.gov/usao-md/pr/former-office-administrator-facing-federal-charges-defrauding-her-employer-more-700000

Former Casino Employee Sentenced To 5 Years Probation For Embezzling $10,000+ - July 7, 2021
https://www.justice.gov/usao-sdms/pr/former-casino-employee-sentenced-theft

Former Accountant Sentenced To Prison For Misappropriating $1.1 Million+ From 4 Employers / Lenders - July 23, 2021
https://www.justice.gov/usao-ndil/pr/accountant-sentenced-more-eight-years-prison-misappropriating-11-million-employers-and

Former Payroll Administrator Found Guilty Of $1.5 Million+ Fraud Against Employer For Over 7 Years - July 23, 2021
https://www.justice.gov/usao-dc/pr/former-payroll-administrator-found-guilty-15-million-fraud-against-longtime-employer

Former School System Technology Coordinator Sentenced To Prison For $336,000+ Wire Fraud / Theft Scheme Per Personal Use - July 23, 2021
https://www.justice.gov/usao-cdil/pr/former-tech-employee-blue-ridge-school-district-sentenced-30-months-imprisonment

Former Bookkeeper For Accounting Firm Pleads Guilty To $670,000 Mail Fraud / Money Laundering Scheme Over 5 Years For Personal Use - July 19, 2021
https://www.justice.gov/usao-edmo/pr/former-bookkeeper-st-louis-accounting-firm-pleads-guilty-670k-fraud-scheme

Former Customer Service Rep. Sentenced To Prison For $11,00 Of Wire Fraud Scheme Over 8 Years - July 13, 2021
https://www.justice.gov/usao-edtx/pr/denton-county-woman-sentenced-15-years-federal-prison-wire-fraud

Administrative Assistant For 2 Non-Profit Organization Sentenced To Prison For Trying To Stealing $200,000+ Of Donor Checks - July 13, 2021
https://www.justice.gov/usao-dc/pr/dc-woman-sentenced-prison-stealing-non-profit-organizations

Former Bookkeeper For Domestic Violence Shelter Pleads Guilty To Stealing $50,000+ Funds For Personal Expenses - Shelter Had To Cease Operations - July 13, 2021
https://www.justice.gov/usao-sdoh/pr/former-bookkeeper-federally-funded-washington-court-house-domestic-violence-shelter

Former Financial Controller Admits To Embezzling $400,000+ From Family-Owned Business - July 21, 2021
https://www.justice.gov/usao-sdca/pr/former-financial-controller-admits-embezzling-almost-half-million-dollars-family-owne-0

Vatican Indicts Cardinal And 9 Others On Multimillion Fraud Charges - July 3, 2021
https://time.com/6077906/vatican-indictment/

CRITICAL INFRASTRUCTURE

2 Cargo Handlers At LAX Aiport Plead Guilty To Conspiracy Charge For Stealing Gold Bars Headed From Australia To New York - July 9, 2021
https://www.justice.gov/usao-cdca/pr/two-cargo-handlers-lax-plead-guilty-conspiracy-charge-stealing-four-gold-bars-headed

WORKPLACE VIOLENCE

Wisconsin Walmart Employee Facing Charges After Repeatedly Punching Elderly Woman - July 13, 2021
https://www.foxnews.com/us/walmart-wisconsin-charges-punched-elderly-woman

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-as-of-july-25-2021/

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)

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 63-year-old, former system administrator that was employed by UBS PaineWebber, a financial services firm, allegedly 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 work stations.

4 years after the attack, UBS was still suffering. Some of the information on the approximately 2,000 Unix-based servers in the home office and the 370 branch offices that were hit by the malicious code were 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)

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 (**2,800+ 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 INCIDENT 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 INCIDENT 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