INSIDER THREAT DEFENSE

Security Behind The Firewall Is Our Business

Insider Threat Incidents

Could They Happen To Your Organization?

The Washington Post

MONDAY, JUNE 10, 2013

Man who leaked NSA secrets steps forward

A REPORTER'S ACCOUNT

To leaker, personal risks were clear

BY BARTON GELLMAN

He called me BRASSBANNER, a code name in the double-barreled style of the National Security Agency, where he worked in the signals intelligence directorate.

Verax was the name he chose for himself, "truth teller" in Latin. I asked him early on, without reply, whether he intended to hint at the alternative fates that lay before him.

Two British dissenters had used the pseudonym. Clement Walker, a 17th-century detractor of Parliament, died in the brutal confines of the Tower of London. Two centuries later, social critic Henry Dunckley adopted "Verax" as his byline over weekly columns in the Manchester Examiner. He was showered with testimonials and an honorary degree.

Edward Joseph Snowden, 29, knew full well the risks he had undertaken and the awesome powers that would soon be arrayed to hunt for him. Pseudonyms were the least of his precautions as we corresponded from afar. Snowden was spilling some of the most sensitive secrets of a surveillance apparatus he had grown to detest. By late last month, he believed he was already "on the X" — exposure imminent.

"I understand that I will be made to suffer for my actions, and that the return of this information to the public marks my end," he wrote in early May, before we had our first direct contact. He warned that even journalists who

SNOWDEN CONTINUED ON A4

Before the world knew his name, tech specialist Edward Snowden, 29, now in Hong Kong, drafted a note of explanation. STORY, A4

Risks of outsourcing
Government reliance on private spying contractors comes with costs as well as benefits. A2

A historic leak
Edward Snowden receives praise and criticism as his name joins that of Daniel Ellsberg. A4

EDWARD SNOWDEN: 'I'M NOT GOING TO HIDE'

Booz Allen consultant could face prosecution

BY BARTON GELLMAN, AARON BLAKE AND GREG MILLER

A 29-year-old man who says he is a former undercover CIA employee said Sunday that he was the principal source of recent disclosures about top-secret National Security Agency programs, exposing himself to possible prosecution in an acknowledgment that had little if any precedent in the long history of U.S. intelligence leaks.

Edward Snowden, a tech specialist who has contracted for the NSA and works for the consulting firm Booz Allen Hamilton, unmasked himself as a source after a string of stories in The Washington Post and the Guardian that detailed previously unknown U.S. surveillance programs. He said he disclosed secret documents in response to what he described as the systematic surveillance of innocent citizens.

In an interview Sunday, Snowden said he is willing to face the consequences of exposure.

"I'm not going to hide," Snowden told The Post from Hong Kong, where he has been staying. "Allowing the U.S. government to intimidate its people with threats of retaliation for revealing wrongdoing is contrary to the public interest."

Asked whether he believes that his disclosures will change anything, he said: "I think they already have. Everyone everywhere now understands how bad things

SURVEILLANCE CONTINUED ON A5

Last Update: March 8, 2017


" The research project of a lifetime
just ran out my . . . USB port!"
Corporate thieves
no longer use the
front door.

Definitions Of Insider And Insider Threat

An Insider is someone who has authorized access to an organization facilities, data, information systems and networks. (Employee, Ex-Employee, Trusted Business Partner, Contractor or Maintenance Personnel)

Insider Threat

A person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities. Other Definitions: (NISPOM Conforming Change 2, National Insider Threat Policy)

Insider Threat Actions

Could intentionally or unintentionally;

- Compromise an organizations security, affecting the confidentiality, integrity and availability of an organizations data, information systems and networks.
- Compromise an organizations ability to protect it's facilities and personnel.

Insider Threat Damages

Can include, but are not limited to;

- Espionage, criminal enterprise, fraud, theft and unauthorized disclosure of information (Classified Information, Sensitive Information, Intellectual Property, Trade Secrets, Personally Identifiable Information (PII))
- Information Technology Sabotage
- Any action that results in the loss or degradation of an organization resources or capabilities and it's ability to accomplish its mission or business function.

INSIDER THREAT HAS MANY DEFINITIONS

- ✓ **Disgruntled Employees**
- ✓ **Workplace Violence / Active Shooter**
- ✓ **Divided Loyalty Or Allegiance To U.S. / Terrorism**
- ✓ **Espionage (National Security, Economic, Industrial, Corporate)**
- ✓ **Data Destruction / Theft, Information Technology Sabotage**
- ✓ **Criminal Activities (Fraud, Financial Theft, Etc.)**
- ✓ **Cyber Criminal - Insider Threat Collusion**
- ✓ **Insiders Who Are: Unwitting, Ignorant, Negligent**
- ✓ **Insiders Who Affect The: Confidentiality, Integrity And Availability Of Information**

INSIDER THREAT OVERVIEW

Insider Threat Defense in conjunction with the National Insider Threat Special Interest Group has complied this report to put an emphasis on just how serious the Insider Threat problem really is. Throughout this document you will see various examples of how damaging and costly an Insider Threat incident can be. Keep in mind that the examples referenced in this document **are only a handful** of the many other "Insider Threat Incidents" we have collected. No government agency, business sector, large or small business in immune from the Insider Threat.

The visibility of the Insider Threat problem has never been greater. The damages that can be caused by an Insider (Witting, Unwittting) can be severe, many times more damaging then an external cyber threat.

The Insider Threat is not just a U.S. Government problem. There have been countless reports of the Insider Threat problem in the private sector and the severe damages that have been caused. The damages from an Insider sabotaging information technology systems or committing theft of an organizations sensitive information, intellectual property, trade secrets, or committing fraud can be very costly.

Insiders have already obtained a badge to access significant portions of an organizations facilities, and a login and password to access significant amounts of an organizations data. Insiders know where the data is stored, and what data has the most value.

Insiders in most cases know what is checked and not checked, and know when they won't be checked or challenged. Insiders attempting to commit a malicious action will in most cases exploit an organizations weakest links, that give them the greatest chance of success, without being caught.

Insider Threat Risk Mitigation requires going beyond compliance regulations and thinking outside the box, because a Malicious Insider most definitely will.

Over the past decade, more than 120 cases of malicious insider crime (Espionage) involving classified national security information were identified by the CERT Insider Threat Center (ITC). The CERT ITC research revealed that malicious insiders exploited business process as often as they exploited technical vulnerabilities. The CERT ITC data analysis also identified more than 100 categories of weaknesses in enterprise architectures that have allowed Insider attacks to occur.

The Insider Threat is a human problem, not just an IT or data loss problem, and needs to be addressed with more then just technology, using a holistic enterprise Insider Threat Risk Mitigation Framework (ITRMF). The ITRMF requires a combination of people, processes, awareness, training, technology and security controls to detect, deter and mitigate Insider Threat risks.

The ITRMF is supported by an Insider Threat Program (ITP). The ITP is comprised of individuals (Trusted Stakeholders) from various departments, business units and supporting functions. Because each organization is unique, the structure of the ITP may be different. The end result for any ITP is the identification of suspicious or malicious activities and behavioral indicators by the Insider, as these are crucial in limiting or neutralizing the potential damage that may be caused by an Insider.

The Insider Threat problem is not just about Malicious Insiders. With such extraordinary advances in technology and Internet connectivity, some CIO's and security professionals are failing to realize that they now have a threat called the Cyber Insider Threat, which is a Non-Malicious Insider. When it comes to cyber threats, countless data breach reports and incidents have shown that most of the problems are the result of the Insider behind the keyboard, who is exhibiting basic human flaws; Ignorance, impatience and gullibility. All these human flaws work hand in hand with the social engineering tactics and phishing e-mails used by cyber criminals. Insiders tend to be too trusting, operating in a “click now, think later” mentality that introduces significant security risks to government agencies and businesses. Cyber Security Awareness and Insider Threat Awareness Training in many organizations are a once a year activity, or in some organizations non-existence.

The Cyber Insider Threat problem was recently outlined in a Government Accountability Office (GAO) report. The report points a finger at "Insider Threats" from federal workers on the government's vast cyber and computer system, joining "foreign nations" as a danger to sensitive and classified information and even personal info.

The GAO also declared frustration with the Obama administration in its new report, over its failure to implement 1,000 security fixes needed to close the door to hackers, inside and out. In testimony to Rep. Barbara Comstock's subcommittee in February 2017, Gregory Wilshusen, director of information security issues for GAO, hit the government for failing to act on 1,000 of 2,500 cybersecurity recommendations it has made.

The GAO report, requested by Rep. Barbara Comstock, the northern Virginia Republican who represents thousands of federal workers, is blunt in its assessment of the threats to cybersecurity.

"Federal systems and networks are also often interconnected with other internal and external systems and networks including the Internet, thereby increasing the number of avenues of attack and expanding their attack surface," said the report.

"Risks to cyber assets can originate from unintentional and intentional threats. These include insider threats from disaffected or careless employees and business partners, escalating and emerging threats from around the globe, the steady advances in the sophistication of attack technology, and the emergence of new and more destructive attacks," it added, pointing a finger to federal insiders.

Insider Threat reports and surveys from various sources continue to provide evidence that we have now entered the era of the "Insider Threat Epidemic".

The Cyber Insider Threat and the Malicious Insider Threat are a **very serious** problem to the U.S. Government and businesses. Until more robust and effective measures are taken by the government and businesses to mitigate the Cyber Insider Threat and the Malicious Insider Threat, you will continue to see countless incidents in the news and in this document.

Businesses especially need to understand that it does not matter who caused a data breach, a Cyber Criminal or Malicious Insider.

Measurable Damage From Data Breaches

A business should pay close attention to a 2017 report that was released from Cicso concerning damages from data breaches. The report provides insights based on threat intelligence gathered by Cisco's security experts, combined with input from nearly 3,000 Chief Security Officers (CSOs) and other security operations leaders from businesses in 13 countries.

According to the Cisco report, organizations that suffered a breach, the effect was substantial: 22% of breached organizations lost customers, 40% of them lost more than a fifth of their customer base, 29% lost revenue, with 38% of that group losing more than a fifth of their revenue, and 23% of breached organizations lost business opportunities, with 42% of them losing more than a fifth of such opportunities.

Far to many times, the NITSIG is seeing businesses trying to understand and identify who causes more damage, a Cyber Criminal or a Malicious Insider. That sad reality is **both** are causing serious damages to businesses on all levels (Loss / Theft of Intellectual Property, Loss of Shareholder Confidence, Loss of Customers, Stock Price Reduction, Etc.)

Hard Facts Regarding Data Breaches - Customers Want Their Data Secured--PERIOD

- Customers don't care whether the data breach is caused by a Cyber Criminal or Malicious Insider. A breach is a breach--PERIOD.
- Customers don't care that your business does not go beyond compliance regulations and "Think Outside The Box. A breach is a breach--PERIOD.
- Customers don't care about how many IT Security Certifications your IT Staff has. A breach is a breach--PERIOD.
- Customers don't care the security posture of your business is weak, and does not have security policies in place to ensure employees and third parties only have the appropriate levels of access to sensitive business data. A breach is a breach--PERIOD.
- Customers don't care that your business does not securely configure your IT systems and networks, lock down USB ports, DVD/CD drives to prevent theft of data. A breach is a breach--PERIOD
- Customers don't care about how much money your business has spent on IT Security Technologies (Firewalls, IDS's, & So Many More), yet they failed to prevent the data breach. A breach is a breach--PERIOD.
- Customer don't care that the IT Security Tools your business purchased are hard to use, not configured correctly for your business, and now are not even used at all. A breach is a breach--PERIOD.
- Customers don't care that your IT Security Team is overloaded with threat intelligence from all your IT Security Technologies. A breach is a breach--PERIOD.
- Customers don't care that your CISO or IT Security Guru fell for the sales pitch from the IT Security Vendor, claiming "Our Tool" will catch that type of attack, but did not. A breach is a breach--PERIOD.
- Customers don't care whether the data is walked out the door by an employee, or it sneaks out past the firewall. A breach is a breach--PERIOD.
- Customers don't care that your employee accidentally clicked on the malicious link, and compromised your company's network and data. A breach is a breach--PERIOD.
- Businesses continue to have excuses for mitigating risks, while Cyber Criminals and Malicious Insiders continue to exploit a businesses **easily** recognizable vulnerabilities -- The Human Exploiting The Human.
- According to a Gartner worldwide Information Security spending grew 7.9% to reach $81.6 Billion in 2016.
- Cyber Criminals in most cases are using social engineering via e-mail phishing attacks and other simple methods that bypass IT Security Technology.
- Malicious Insiders in most cases exploit a businesses vulnerabilities, that are overlooked or ignored, that IT Security Tools will not fix.
- Until businesses stop trying to use IT Security Technologies as a band aid and quick fix to the data breach problem, businesses will experience data breaches that are very costly and damaging, as shown in the rest of this document.

INSIDER THREAT PROGRAM SUCCESS

Developing, implementing and managing a **successful** Insider Threat Program is possible. Once an organization can get beyond the hurdles of establishing an Insider Threat Program, the benefits of protecting an organization will be visible.

Coast Guard Insider Threat Program - July 13, 2016

Since the Coast Guard fully stood up its Insider Threat Program, it's detected and prevented multiple threats. Most were non-malicious in nature, and ranged from system administrator abuse to password sharing.

A DHS technical monitoring solution audited 33 million actions on the department's enterprise classified networks in this fiscal year, Gen. Frank Taylor, undersecretary for intelligence and analysis at DHS, told the committee.

Roughly 215,000 of those actions required manual review from DHS analysts, and 72 of those led to further investigations.

Taylor said the DHS Insider Threat Program identified 162 violations and supported 15 counterintelligence and internal investigations during the previous two fiscal years.

Source:

http://federalnewsradio.com/technology/2016/07/coast-guard-says-first-achieve-foc-insider-threat-program/

TERRORISM

DC Metro Transit Cop Appears In Court for Allegedly Trying to Assist ISIS - August 3, 2016

A veteran police officer with one of the nation's most prominent transit systems appeared in federal court today in connection to charges that he tried to help ISIS.

Authorities believe that officer Nicholas Young, while working for the Metro Transit Police Department in Washington, D.C. — a community he swore to protect — was trying to assist ISIS operatives find more ways to communicate in secret. Young allegedly purchased technology-related items to send to the ISIS operatives so they could evade authorities when contacting one another.

Instead of allegedly engaging with true ISIS associates, however, Young was actually in touch with FBI informants and agents from the FBI's Joint Terrorism Task Force in Washington, which has been conducting a long undercover investigation in the case, officials said.

Source:

http://abcnews.go.com/US/dc-metro-transit-cop-appears-court-allegedly-assist/story?id=41089376

Orlando Shooter Killed 50 People - Indicators Present, But Ignored - June 13, 2016

The security company that employed Orlando nightclub shooter Omar Mateen also is a federal contractor for the Homeland Security and State departments -- raising more questions about how he passed background checks despite being on the FBI's radar screen and the level of security at a firm handling sensitive U.S. operations.

At least one former G4S employee, Daniel Gilroy, says he raised numerous concerns with supervisors about Mateen's hateful and potentially dangerous behavior.

Gilroy told Fox News that he and Mateen had worked as security guards at the same South Florida resort and that Mateen, a Muslim, used "horrible words" at the sight of women and blacks and was in a constant state of "anger and rage."

However, the company refused to take action on his complaints, and Gilroy was forced to quit last year after Mateen began sending him harassing text and phone messages, according to Florida Today.

"The company wouldn't do anything," Gilroy told the paper. "This guy was unhinged and unstable. He talked of killing people."

He said co-workers were concerned about "inflammatory and contradictory" statements he had made, including claiming family connections to Al Qaeda. Mateen later admitted making the statements but said he did so out of anger because he thought his co-workers were discriminating against him. The FBI closed the preliminary investigation, before briefly looking at him one more time in 2014.

Source:

http://www.foxnews.com/politics/2016/06/13/orlando-killer-worked-for-dhs-state-contractor-that-helps-secure-us-embassies.html?utm_source=360Works%20CloudMail&utm_medium=email&utm_campaign=NewsWatch

And Many More.....

AIRPORT / AVIATION

Increasing Concern About Insider Threats At US Airports - House Homeland Security Committee Report - February 6, 2017

The House Homeland Security Committee Majority Staff has issued a report entitled 'America's Airports: The Threat From Within' that examines employee screening at the approximately 450 airports in the U.S. under federal control and found that "much more needs to be done to improve the state of access controls and mitigate the insider threat facing America's aviation sector."

According to the 21-page report: Approximately 900,000 people work at these airports, and many are able to bypass traditional screening requirements that travelers visiting the airports must endure. While the overwhelming majority of these airport workers take the inherent responsibility seriously, there are increasing concerns that insider threats to aviation security are on the rise.

The report – the result of an investigation conducted by Transportation and Protective Security Subcommittee – continued: The Subcommittee has worked closely with the Transportation Security Administration (TSA) and the aviation stakeholder community to examine how we can work together to improve access controls and employee screening at our nation's airports.

"The recommendations outlined in this report, along with the requirements of the Aviation Employee Screening and Security Enhancement Act of 2017, which I introduced today, will serve as a roadmap for TSA, airports, and air carriers to close security vulnerabilities at our nation's airports," Subcommittee Chairman John Katko (R-NY) stated in a press release about the report.

The Subcommittee "found that a majority of airports do not have full employee screening at secure access points" and that these airports "are unable to demonstrate the security effectiveness of their existing employee screening efforts, which consist largely of randomized screening by TSA officers or airport law enforcement personnel," according to the press release.

The report made nine recommendations that include examining the costs and feasibility of expanded employee screening, educating aviation workers on their role in mitigating insider threats, targeting the use of employee screening to be more strategic, and implementing the Federal Bureau of Investigation's (FBI) RapBack Service for all credentialed aviation worker populations.

Recent examples of insider threats discussed in the report include an attempt to detonate a bomb at an airport, gun and drug smuggling, and employees who became involved in terrorist activities overseas. The complete "America's Airports: The Threat From Within" report is available online.

Source:
http://abcnews.go.com/US/increasing-concern-insider-threats-us-airports-govt-report/story?id=45308790

TSA Workers Helped Puerto Rico-Based Ring Smuggle $100M Of Cocaine For Over A Decade, Prosecutors Say - February 13, 2017

Prosecutors in Puerto Rico have smashed a ring of current and former U.S. Transportation Security Administration workers that allegedly smuggled 20 tons of cocaine worth as much as $100 million into the U.S. over more than a decade.

A dozen members of the alleged ring, including TSA workers and airport employees, were indicted Feb. 8 in the District of Puerto Rico on charges of conspiracy to possess with intent to distribute cocaine, U.S. Attorney for the District of Puerto Rico Rosa Emilia Rodríguez-Vélez announced. "These individuals were involved in a conspiracy to traffic massive quantities of illegal narcotics to the continental United States," Rodríguez-Vélez said.

Authorities said the federal employees used their positions as TSA baggage screeners to wave massive amounts of coke through security. The charges point to an insider threat, a congressional source told Fox News, saying the suspects could have smuggled explosives instead of drugs.

Beginning in 1998, some three years before the formation of the TSA, the suspects allegedly smuggled suitcases containing up to 15 kilograms of cocaine through the TSA security system at the Luis Muñoz Marín International Airport in San Juan, prosecutors said. As many as five "mules," or human smugglers, were used on each flight, with each checking in up to two suitcases, according to authorities. During the 18-year conspiracy, the suspects sent 20 tons of cocaine into the U.S., according to prosecutors.

Source:
http://www.foxnews.com/us/2017/02/13/tsa-workers-helped-puerto-rico-based-ring-smuggle-100m-cocaine-prosecutors-say.html

Fatal Descent Of Germanwings Plane Was 'Deliberate,' French Authorities Say - March 26, 2015

French investigators say that the 27-year-old co-pilot of the Germanwings flight, Andreas Lubitz, deliberately crashed the plane, an Airbus A320, after locking the captain out of the cockpit. Mr. Lubitz and the 149 others on the flight, from Barcelona, Spain, to Dusseldorf, Germany, were killed.

Prosecutors in France and Germany have said Mr. Lubitz had a history of severe depression and in the weeks leading up to the crash had sought out numerous doctors for treatment of anxiety, sleeplessness and a perceived problem with his vision.

Lubitz had seven medical appointments within the month before the March 24 crash, including three appointments with a psychiatrist, Robin said. Some of the doctors felt Lubitz was psychologically unstable, and some felt he was unfit to fly, but "unfortunately that information was not reported because of medical secrecy requirements," the prosecutor said.

In Germany, doctors risk prison if they disclose information about their patients to anyone unless there is evidence they intend to commit a serious crime or harm themselves.

Source:

http://www.cbsnews.com/news/doctors-felt-germanwings-co-pilot-andreas-lubitz-unfit-to-fly-prosecutor-says/
http://www.nytimes.com/news-event/germanwings-flight-9525-crash?inline=nyt-org

6 Other Times Commercial Pilots Were Suspected Of Crashing Planes On Purpose

Source:

http://www.huffingtonpost.com/2015/03/26/pilots-crashing-on-purpose_n_6948448.html

Airport Security Seizes 70 Pounds Of Cocaine From Airline Employee - March 24, 2016

Authorities said a JetBlue flight attendant used her credentials to attempt to carry the cocaine through airport security in Los Angeles on Friday. But when the Transportation Security Administration selected the woman for a random security screening, she took off her heels and ran away. Marsha Gay Reynolds surrendered to authorities Wednesday at John F. Kennedy International Airport in New York.

Source:

http://www.syracuse.com/politics/index.ssf/2016/03/airport_seizes_70_pounds_of_cocaine_exposes_failure_to_curb_insider_threat_katko.html

Aviation Security Advisory Committee: Employee Screening Working Group Report - April 8, 2015
Source:
https://www.tsa.gov/sites/default/files/asac-employee-screening-working-group-04-15.pdf

The Insider Threat Is Real: Gaps In Airport Security Highlighted In NBC News Video - November 25, 2015
At New York's John F. Kennedy International Airport, used by more than 50 million passengers every year, NBC News' cameras captured employees simply swiping their electronic key cards to get into the facility this week. NBC News also obtained video from earlier this year that showed the same thing.
Source:
http://www.nbcnews.com/news/us-news/insider-threat-real-gaps-airport-security-highlighted-new-video-n469701

DHS IG Report On TSA Insider Threat Problem - September 2012
Source:
https://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-120_Sep12.pdf

Chicago Airport Fire Started By Employee - 2014

In the early morning hours of September 26, 2014, the Federal Aviation Administration's (FAA) Chicago Air Route Traffic Control Center (ARTCC) declared "ATC Zero" after an employee of the Harris Corporation deliberately set a fire in a critical area of the facility. The fire destroyed the Center's FAA Telecommunications Infrastructure (FTI) system – the telecommunications structure that enables communication between controllers and aircraft and the processing of flight plan data.

The fire at Chicago Center and its after effects inconvenienced passengers, reportedly cost the airlines over $350 million dollars and raised questions about the resiliency of our National Airspace System and its ability to withstand a similar systematic attack in the future.

FAA contractor Brian Howard pleaded guilty in May to setting the fire in an outburst targeting his employer and government workers he thought were "lazy." He was sentenced in September to 12 1/2 years in prison

According to the repot, Howard's last scheduled shift at the Aurora facility was Sept. 18, 2014. According to court filings, Howard walked into the radar facility before dawn on Sept. 26, 2014, carrying a gas can, a lighter and knives; he cut cables and set fire to a telecommunications room before trying to slit his throat. The disruption forced an hours long shutdown of Chicago's airports and the center didn't reopen for two weeks. Thousands of flights were canceled.

The inspector general's report contends that at the time of the fire, security wasn't able to deal with an insider threat to the air traffic system. It says the FAA didn't have a way to block a current or former employee from accessing the facility; for example, there was no requirement that an employee's access card be deactivated if he or she was transferred to a new facility.

Source:

http://www.faa.gov/news/media/ZAU_Fire_Public_Review.pdf
https://www.oig.dot.gov/sites/default/files/FAA%20contingency%20plans%20and%20security%20protocols%20at%20Chicago%20ATC%20facilities.pdf
http://bigstory.ap.org/article/b94f2378bba843c5a133fe4a33ead714/report-slams-faa-response-fire-air-traffic-facility
http://www.cbsnews.com/news/report-slams-faa-response-to-fire-at-chicago-air-traffic-facility/

WORKPLACE VIOLENCE

Unfortunately very disgruntled employees Insiders have resorted to workplace violence, in some cases resulting in the deaths of innocent coworkers..

According to the Occupational Safety and Health Administration (OSHA), approximately

- 2 million employees are victims of workplace violence each year.
- 18% of violent crimes are committed at the workplace, and roughly 800 workplace homicides occur each year.
- Between January 2009 and July 2015, there were 133 mass shootings in the workplace and shootings account for 78 % of all workplace homicides. (Source)

Violence in the workplace must be a top concern for employers, as no organization is immune from workplace violence and no organization can completely prevent it.

The National Insider Threat Special Interest Group has complied a disturbing amount of "Workplace Violence" incidents in a on-line magazine they publish.

A company that ignores the warnings signs could face legal action.
Jury Awards Over $1 Million In Negligent Hiring Lawsuit Involving Workplace Violence

Family Of Security Guard Killed By Disgruntled Employee, Sues Labor Department For $10 Million - February 14, 2017

A security guard gunned down by a disgruntled ex-U.S. Department of Labor employee died an "entirely preventable" death — because nobody warned him the former staffer was dangerous, a new $10 million lawsuit alleges.

Onetime Labor Department worker Kevin Downing walked into the federal office building on Varick and Houston streets around 5 p.m. on Aug. 21, 2015, and fatally shot security guard Idrissa Camara, 53, in the head before turning the gun on himself.

Camara's family claims in a new lawsuit that Downing, 68, "was a well-known danger" who had made such serious threats that the Labor Department and General Services Administration — which runs operations at federal buildings — posted an extra security guard outside the Labor Department's eighth-floor offices.

But the father of three, who came to the U.S. from the Ivory Coast in 1991, "was never warned of the threat" — even though he was stationed at the security checkpoint on the ground floor, where his "primary job responsibility was to protect the building," the suit claims.

Neither government agency gave Camara, nor other guards on the ground floor, a photo or description of Downing, They also didn't tell his security firm to warn the guards about him, according to court papers.

Source:

http://www.nydailynews.com/new-york/family-security-guard-killed-job-sues-labor-department-article-1.2972631

NATIONAL SECURITY DATA BREACHES

NSA Contractor Allegedly Stole 50 Terabytes Of Data Over 20 Years - October 20, 2016

Federal prosecutors in Baltimore, Maryland said they will charge a former National Security Agency contractor with violating the Espionage Act, alleging that he made off with "an astonishing quantity" of classified digital and other data over 20 years in what is thought to be the largest theft of classified government material ever.

In a 12-page memo, U.S. Attorney Rod Rosenstein and two other prosecutors laid out a much more far-reaching case against Harold T. Martin III than was previously outlined. They say he took at least 50 terabytes of data and "six full banker's boxes worth of documents," with many lying open in his home office or kept on his car's back seat and in the trunk. Other material was stored in a shed on his property.

Three extremely disturbing facts were revealed in the court filings. First, Martin took hand written notes on printed classified documents that appear to have been explaining the context of the documents to an outsider. Second, forensic artifacts suggest he communicated in Russian language on his computer. Finally, investigators recovered a letter Martin wrote in 2007 to his coworkers which makes him appear extremely disgruntled. All of these items seem to bolster the government's case for pretrial confinement.Martin also took personal information about government employees as well as dozens of computers, thumb drives and other digital storage devices, the government memo said.

Though he lacks a valid U.S. passport, the government said Martin could still flee to a foreign government that might wish to help him. Prosecutors said he has communicated with unnamed people in Russian and in June downloaded information on Russian and other languages.The prosecutors also said Martin had an "arsenal" of weapons in his home and car, including an assault-rifle-style tactical weapon and a pistol-grip shotgun with a flash suppressor.

Martin allegedly used a "sophisticated software tool which runs without being installed on a computer and provides anonymous Internet access, leaving no digital footprint on the Machine," and he tried "to run operating systems on his machines that would not leave any forensic evidence of his computer activities." That could suggest Martin was using TAILS or another USB-bootable operating system in conjunction with Tor or a VPN.

Source:

https://www.washingtonpost.com/world/national-security/government-alleges-massive-theft-by-nsa-contractor/2016/10/20/e021c380-96cc-11e6-bb29-bf2701dbe0a3_story.html

WikiLeaks Data Breach (Source)

U.S. soldier Bradley Manning was sentenced on Wednesday to 35 years in a military prison for turning over more than 700,000 classified files to WikiLeaks in the biggest breach of secret data in the nation's history.

NSA Data Breach (Source)

In June 2013 Edward Snowden an NSA contractor leaked very highly classified documents on NSA's Surveillance Programs. Snowden is responsible for one of the most significant leaks in U.S. political history. Snowden is a 29-year-old former technical assistant for the CIA and who worked for defense contractor Booz Allen Hamilton at the time of the data breach. Snowden has since fled the U.S.

Other Trusted Insiders Gone Bad

Abujihaad	Hasaan	Navy - United States
Al Halabi	Ahmad	Air Force - United States
Allen	Michael	Navy - United States
Ames	Aldrich	Central Intelligence Agency (CIA)
Anderson	Ryan	Army - National Guard
Anzalone	Charles	Marine Corps
Aragoncillo	Leandro	Federal Bureau of Investigation (FBI)
Baba	Stephen	Navy - United States
Bell	William	Hughes Aircraft
Bergersen	Gregg	Department of Defense
Best	Gregor	Air Force - United States
Boeckenhaupt	Herbert	Air Force - United States
Boone	David	National Security Agency
Borger	Harold	Department of Defense
Butenko	John	International Electronic Company
Carney	Jeffrey	Air Force - United States
Cascio	Guiseppe	Air Force - United States
Charlton	John	Lockheed Martin Corporation
Chin	Larry	Central Intelligence Agency (CIA)
Chung	Dongfan	Boeing Company
Clark	James	Department of State
Coberly	Alan	Marine Corps
Colepaugh	William	Naval Reserve - United States
Conrad	Clyde	Army - United States
Cooke	Christopher	Air Force - United States
Cordrey	Robert	Marine Corps

Davies	Allen	Air Force - United States
Davila	Rafael	Army - National Guard
DeChamplain	Raymond	Air Force - United States
Dedeyan	Sahag	Johns Hopkins Applied Physics Laboratory
Diaz	Matthew	Navy - United States
Dolce	Thomas	Army - United States
Drummond	Nelson	Navy - United States
Ellis	Robert	Navy - United States
Farnsworth	John	Navy - United States
Fondren	James	Department of Defense
Ford	Kenneth	National Security Agency
Franklin	Lawrence	Department of Defense
French	George	Air Force - United States
Gessner	George	Army - United States
Gowadia	Noshir	Northrop Corporation
Graf	Ronald	Navy - United States
Greenglass	David	Army - United States
Groat	Douglas	Central Intelligence Agency (CIA)
Grunden	Oliver	Air Force - United States
Haguewood	Robert	Navy - United States
Hall	James	Army - United States
Hamilton	Frederick	Defense Intelligence Agency
Hanssen	Robert	Federal Bureau of Investigation (FBI)
Harris	Ulysses	Army - United States
Helmich	Joseph	Army - United States
Horton	Brian	Navy - United States

INSIDER THREATS - WHAT THE MEDIA DOES NOT COVER

HOW DAMAGING CAN AN INSIDER THREAT INCIDENT BE?

Low-Level Engineer Steals $1 Billion Worth Of Intellectual Property

A low-level engineer managed to steal $1 billion (yes, that is with a 'b') worth of intellectual property. The engineer resigned his position working for a major microprocessor manufacturer to go to work for a competitor. While still employed by the victim and supposedly using remaining vacation time, he went to work for the competitor. His access to the victim's computer systems were not terminated until a week after he started with the competitor. During this period, the engineer downloaded 13 "top secret" (internal classification) documents from his soon to be former employer. The documents contained details on the process for developing next generation microprocessors.
http://regmedia.co.uk/2008/11/06/amdintelpaniindictment.pdf

Major European Company Says Employee Has Gone Missing With $100M - Feb. 22, 2017

Power and robotics firm ABB (ABB) announced Wednesday that it has "uncovered a sophisticated criminal scheme" at its South Korean unit. It only noticed the huge sums had been stolen after the employee of the subsidiary disappeared about two weeks ago.

The employee, who ABB has not identified, is suspected of forging documents and working with individuals outside the company to steal the money, according to ABB and South Korean police.

A police spokesman said that the suspect is believed to have fled to Hong Kong and that they are working with Interpol to bring him back to South Korea. Interpol declined to comment on the investigation.

The embezzlement and misappropriation of funds is limited to South Korea, where ABB employs about 800 staff, the company said. Other people could still come under investigation.

Source:
http://money.cnn.com/2017/02/22/news/companies/abb-criminal-activity-south-korea/index.html

Bangladesh $81 Million Bank Heist Probe Finds 'Negligent' Insiders - December 9, 2016

An internal investigation into the February theft of $81 million from the central bank of Bangladesh reportedly found that a handful of negligent and careless bank officials inadvertently helped facilitate the heist by outside hackers.

"They were negligent, careless and indirect accomplices," he told Reuters, adding that attackers had exploited vulnerabilities in the bank's information security defenses. "The committee came to the conclusion that the heist was essentially committed by external elements."

http://www.govinfosecurity.com/bangladesh-bank-heist-probe-finds-negligent-insiders-a-9586

CEO Fired After Falling For Fake CEO E-Mail Scam - Cost Company $47 Million - May 26. 2016

FACC's board on Wednesday fired Walter Stephan, CEO of the Boeing and Airbus supplier, due to errors made in connection with what it called a “president fraud incident” that the firm discovered in January.FACC said Stephan’s role had been revoked with “immediate effect” because he had “severely violated his duties, in particular in relation to the ‘Fake President Incident’.”

'The attackers tricked FACC financial controllers into wiring $47 Million to fraudsters during what appears to be several transactions. FACC said that its share price had fallen 38% since the incident.

Source:

http://www.cso.com.au/article/600535/ceo-fired-after-fake-ceo-email-scam-cost-firm-47m/

Cyberheist Nets $44 Million In Single CEO Fraud Attack - September 2016

According to authorities, a young woman working as CFO at Leoni's Bistrita factory was the target of the scam, when she received an email spoofed to look like it came from one of the company's top German executives. She then proceeded paying out $44 million in the process.

According to the Romanian Directorate for Investigating Organized Crime and Terrorism (DIICOT), the scammers had extensive knowledge about the internal procedures for approving and processing transfers at Leoni, meaning the network had been penetrated earlier, highly likely through phishing emails, and the bad guys had been doing recon for months.

Source:

https://blog.knowbe4.com/cyberheist-nets-44-million-in-single-ceo-fraud-attack

IT Systems Administrator Receives Poor Salary Bonus - Sabotages IT Systems - December 13, 2006

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. The malicious code he used is said to have cost UBS $3.1 million in recovery expenses and thousands of lost man hours. He was apparently irate about a poor salary bonus he received of $32.000. He was expecting $50.000. In retaliation, he wrote a program that would delete files and cause disruptions on the UBS network. His 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:

http://www.informationweek.com/ex-ubs-systems-admin-sentenced-to-97-months-in-jail/d/d-id/1049873?

And Many More.....

POOR SECURITY PRACTICES

Fired IRS Employees Don't Always Have Access Revoked - July 7, 2016

The Internal Revenue Service can't always be sure that former employees' access to systems and buildings has been revoked, according to a recent report.

The Treasury Inspector General for Tax Administration estimates that the IRS could not verify that all security items were recovered from over two-thirds (66 percent) of the approximately 4,100 employees who left from the IRS during fiscal year 2014. This includes 186 who departed during a pending disciplinary case, including criminal misconduct.

TIGTA said that the IRS controls to verify that physical access to government facilities is secured when employees leave -- including a computer process that documents if security items are recovered from them -- were not effective in preventing access to government facilities and computers after employees separated.

The inspector general also reviewed a sample of 10 employees who left during pending disciplinary cases, and found that the IRS could not verify the recovery of the security items for six of these employees and could not provide evidence that these cases were referred to the TIGTA Office of Investigations, as required. Some of the uncollected security items were later used.

Source:

http://www.accountingtoday.com/news/tax-practice/fired-irs-employees-dont-always-have-access-revoked-78616-1.html

And Many More.....

SOCIAL ENGINEERING - IT JUST TAKES ONE MOUSE CLICK

The Inside Story Of The Biggest Hack In History (Caused By Insider) - August 9, 2015

It was known inside the InfoSec community, but now more details have been made public through CNN after a BlackHat 2015 presentation. Until now, little of this was publicly known. But Chris Kubecka, a former security advisor to Saudi Aramco after the hack, spoke to CNN Money about her experience.

Three years ago, the world witnessed the worst hack ever seen on Saudi Aramco, one of the world's largest oil companies.

It started sometime in mid-2012. One of the computer technicians on Saudi Aramco's information technology team opened a scam email and clicked on a bad link.

In a matter of hours, 35,000 computers were partially wiped or totally destroyed. Without a way to pay them, gasoline tank trucks seeking refills had to be turned away. Saudi Aramco's ability to supply 10% of the world's oil was suddenly at risk.

U.S. intelligence officials believe the attackers to be Iranians, and they did not just erase data on 35,000 Saudi Aramco computers; they replaced the data with an image of a burning U.S. flag. And one of the most valuable companies on Earth was propelled back into 1970s technology, using typewriters and faxes. When it comes to sheer cost, the recent cyberattacks on Sony Pictures and the American government pale in comparison.

Source:

http://blog.knowbe4.com/the-inside-story-of-the-biggest-hack-in-history
http://money.cnn.com/2015/08/05/technology/aramco-hack/

And Many More.....

EMPLOYEE OUTSOURCES JOB

Software Developer Outsourced Job To China Over VPN - January 16, 2013

In one exemplary 2013 illustration of employee negligence, an American software developer outsourced his programming job to a consulting firm in Shenyang, China for approximately $50,000 while he continued to collect a salary of several hundred thousand dollars. Meanwhile, the negligent insider spent his workdays surfing social media and reading emails.

When the company checked his web-browsing history, a typical "work day" for Bob was: 9am, arrive and surf Reddit for a couple of hours, watch cat videos; 11.30am, take lunch; 1pm, eBay; 2pm-ish, Facebook updates, LinkedIn; 4.40pm–end of day, update email to management; 5pm, go home.

The insider activity was detected when an investigation into anomalous activity discovered that the employee's credentials were being used to remotely access the company systems. The employee had mailed his multi-factor authentication key to the Chinese consultant via Fed-Ex.

For the potential years that the employee outsourced his job, he received excellent marks in his performance reviews and the clean and functional code that he submitted was considered some of the best in the organization.

The employee, whom was in his mid-40s, a "family man, inoffensive and quiet. Someone you wouldn't look twice at in an elevator."

The evidence, said Valentine, even suggested he had the same scam going across multiple companies in the area.

Source:

http://www.bbc.com/news/technology-21043693

https://www.theguardian.com/world/2013/jan/16/software-developer-outsources-own-job

And Many More.....

INSIDER THREAT COLLUSION

Defense Contractor Cheating The Navy's 7th Fleet Is The Largest Corruption Scandal Ever - December 27, 2016
This story makes the Bradley Manning and Edward Snowden incidents look minor compared to this. This is the worst corruption scandal in Navy history. This is Insider Threats Gone Wild.

What this defense contractor was doing was clearly wrong on the surface (Overbilling). But when politics, bribes, prostitutes, cash, vacations, gifts, parties, insider moles-paid informants, etc. are involved, people look the other way. This scandal also involved the This incident involved the; unauthorized disclosure of classified information

The contractor was Glenn Defense Marine Asia, who provided port security for Navy ships and submarines. This investigation started in 2006. It took the NCIS-Navy 10 years to finally nail this defense contractor. So many Navy people were involved in this scandal. 12 people, including a Navy Admiral, and 9 other Navy personnel have pleaded guilty. 5 people still face charges. Close to 200 other individuals are under scrutiny. Among them are about 30 current of retired Navy Admirals.
Source

Federal Authorities Charge 33 U.S. Postal Services Employees For Theft, Bank Fraud, Conspiracy, Embezzlement - August 26, 2016
Thirty-three defendants were charged as part of a sweep targeting criminal activity that has victimized the United States Postal Service (USPS) and its customers. Most of the defendants charged as part of the sweep are USPS employees who allegedly stole mail, embezzled from the agency or, in one case, failed to deliver nearly 50,000 pieces of mail.
Source:
https://www.justice.gov/usao-cdca/pr/federal-authorities-charge-33-people-crimes-against-us-postal-service-including-theft

Dark Web Recruiters Target Insiders & Employees - February 1, 2017

According to a report from RedOwl and IntSights, the recruitment of insiders within the Dark Web is active and growing, with forum discussions and insider outreach nearly doubling from 2015 to 2016.

Sophisticated threat actors use the Dark Web to find and engage insiders to help place malware behind an organization's perimeter security. Insiders then use these underground forums to "cash out" on their services through insider trading and payment for stolen credit card information.

The puppet-masters are also able to arm insiders with the tools and knowledge necessary to help steal data and commit fraud, among other acts, and also to cover any tracks. In one instance, a hacker solicited bank insiders to plant malware directly onto the bank's network. This approach significantly reduces the cost of action as the hacker doesn't have to conduct phishing exercises and can raise success rates by bypassing many of the organization's technical defenses (e.g. anti-virus or sandboxing).

The lures are significant. On one forum, the attacker explained the approach to a potential collaborator, indicating that he needs direct access to computers that access accounts and handle wire transfers, and that he offers to pay "7 figures on a weekly basis" for continued access.

Source:
https://www.infosecurity-magazine.com/news/dark-web-recruiters-target/

VA Hospital Employees Stealing Drugs Intended For Patients - February 29, 2017

Federal authorities are stepping up investigations at Department of Veterans Affairs medical centers due to a sharp increase in opioid theft, missing prescriptions or unauthorized drug use by VA employees since 2009, according to government data obtained by The Associated Press. Doctors, nurses or pharmacy staff at federal hospitals — the vast majority within the VA system — siphoned away controlled substances for their own use or street sales, or drugs intended for patients simply disappeared.

Aggravating the problem is that some VA hospitals have been lax in tracking drug supplies. Congressional auditors said spot checks found four VA hospitals skipped monthly inspections of drug stocks or missed other requirements. Investigators said that signals problems for VA's entire network of more than 160 medical centers and 1,000 clinics, coming after auditor warnings about lax oversight **dating back to at least 2009.**

Source:

http://www.presstelegram.com/government-and-politics/20170220/are-va-hospital-employees-stealing-drugs-intended-for-patients

And Many More.....

CRITICAL INFRASTRUCTURE

In April 2011, a lone water treatment plant employee allegedly manually shut down operating systems at a wastewater utility in Mesa, Arizona in an attempt to cause a sewage backup to damage equipment and create a buildup of methane gas. Automatic safety features prevented the methane buildup and alerted authorities, who apprehended the employee without incident.

In January 2011, a recently fired employee from a US natural gas company allegedly broke in to a monitoring station of his ex-employer and manually closed a valve, disrupting gas service to nearly 3,000 customers for an hour.

In 2009, a disgruntled former information technology employee of a Texas power plant allegedly disrupted the company's energy-forecast system when the company failed to deactivate the employee's account access and confiscate his company-issued laptop after firing him weeks earlier. The cyber intrusion resulted in a $25,000 loss to the company.

In 2000, a contract employee, who became disgruntled after being turned down for a permanent position at an Australian wastewater services company, used his insider access and expertise to attack the facility's supervisory control and data acquisition (SCADA) systems. The attack disabled system functions and allowed a total of 800,000 liters of untreated sewage to spill into receiving waters over a period of several weeks.

A US citizen who was arrested in Yemen in a March 2010 roundup of suspected al-Qaeda members worked for several contractors performing non-sensitive maintenance at five different US nuclear power plants from 2002 to 2008. This individual was able to pass federal background checks, as recently as 2008, before becoming a contracted employee.

And Many More.....

IT SABOTAGE

Fired IT Employee Demands $200K In Exchange For Unlocking Data - January 18, 2017

A fired IT employee demanded his former employer pay him 200,000 USD in exchange for the return of its sensitive information.

Triano Williams hired attorney Calvita J. Frederick to represent him in a dispute involving the American College of Education, an Indianapolis-based online provider of Master's and Doctorate degrees in teaching at which he previously worked.

The disagreement involving Williams and the school date back to early 2016. At that time, Williams was one of many IT employees for the college spread across the country. In a move to centralize its operations, the American College of Education asked that all IT employees relocate to Indianapolis or resign and take a severance deal.

Williams couldn't relocate because he says he maintains joint custody of his daughter in Chicago. But he also refused to resign. The school kept Williams on as the sole IT administrator until they fired him on 1 April 2016.

Before he left, however, the employee changed the administrative password on a Google account owned by the school. That account stored email and course material for over 2,000 students at the college. Without access to the account, those students couldn't view their papers or use their school-issued emails.

The American College of Education asked if Google could provide them with access to the account. Google said it could only restore access to Williams, the account's owner. When the school contacted Williams, that's when his lawyer sent over the letter.

For its trouble, the college filed a case against Williams in Indiana. The man failed to appear at multiple hearings in Indianapolis, which led Superior Judge Heather Welch to issue a default judgment in September ordering Williams pay the college 248,350 USD in damages.

Source:

http://www.tripwire.com/state-of-security/latest-security-news/fired-employee-demands-200k-exchange-unlocking-data/#.WH90Yiy7-lM.twitter

Former Citibank Employee Sentenced For Shutting Down 90% Of Firm's Network - July 28, 2016

A former Citibank employee was sentenced to 21 months in prison after wiping routers and shutting down 90 percent of the firm's network access across North America.

In February 2016, Dallas resident Lennon Ray Brown admitted to damaging a protected Citibank computer in 2013 by transmitting a code and command that erased the running configurations of 10 core Citibank Global Control Center routers, according to a July 25 Justice Department press release.

At the sentencing, the government read a text Brown sent shortly after the attack explaining his motive. "They was firing me. I just beat them to it," the text read. "Nothing personal, the upper management need to see what they guys on the floor is capable of doing when they keep getting mistreated."

Source:

http://www.scmagazine.com/former-citibank-employee-sentenced-to-21-months-for-wiping-firms-routers/article/512543/

IT Administrator Sabotages Network / PBX System - January 28, 2014

When EnerVest IT Administrator Ricky Joe Mitchell heard that his job with the oil and gas company was on the chopping block, he didn't go quietly. Instead, he reset the company's servers to their original factory settings, disabled cooling equipment for EnerVest's IT systems, along with a data-replication process and deleted PBX system info. As a result, EnerVest was unable to communicate reliably with customers or conduct business operations for a full month and was forced to spend hundreds of thousands of dollars on data recovery efforts. The incident cost the company over $1 million, according to the prosecution. In addition data that the company thought had been backed up, could not be retrieved.

Mitchell will be sentenced on April 24, 2014 to a maximum term of imprisonment of ten years and three years supervised release. Mitchell will also be ordered to pay restitution for the damage caused by his criminal conduct. The U.S. Secret Service conducted the investigation.

Source:

https://www.justice.gov/usao-sdwv/pr/former-network-engineer-pleads-guilty-crashing-employers-computer-system

IT Systems Administrators Sabotage Cost $10 Million+ And As A Result Had To Lay Off 80 Employees

An angry systems administrator—who alone developed and managed his company's network—centralized the software that supported the company's processes on a single server. He then coerced a coworker to give him the only backup tapes for the software. After the systems administrator was fired for inappropriate and abusive treatment of his coworkers, a logic bomb he had planted deleted the only remaining copy of the critical software from the company's server. The company estimated the cost of damage in excess of $10 million and as a result had to lay off 80 employees.

A former IT consultant who caused $1.2 million (Australian) in damages to his former employer by deleting more than 10,000 user accounts on government servers. The man was trying to demonstrate security vulnerabilities in the systems; he was also drunk and upset that his fiancé had broken off their engagement.
http://www.theregister.co.uk/2009/03/13/nt_hack_convict

A former network administrator changed passwords on a city FiberWAN and refused to disclose the new passwords to administrators leaving the city without administrative control of the network for 12 days.
http://www.computerworld.com/s/article/9176060/Childs_found_guilty_in_SF_network_password_case

Management Information Systems (MIS) professional at a military facility learns she is going to be let go due to downsizing. She decides to encrypt large parts of the organization's database and hold it hostage. She contacts the systems administrator responsible for the database and offers to decode the data for ten thousand dollars in "severance pay" and a promise of no prosecution. The organization agrees to her terms before consulting with proper authorities. Prosecutors reviewing the case determine that the administrator's deal precludes them from pursuing charges.

And Many More.....

UN-AUTHORIZED DISCLOSURE / DATA BREACHES / DATA THEFT ESPIONAGE / TRADE SECRET THEFT / FINANCIAL FRAUD / EMBEZZLEMENT / BRIBERY AND MORE.....

Pfizer Sues Ex-Marketing Director Over Trade Secret Theft - February 28, 2017

Pfizer Inc. on Tuesday accused a former global marketing director who voluntarily resigned in January of misappropriating the company's trade secrets, asking a Pennsylvania federal judge for an emergency restraining order to protect the information.

The company said that Aimee De Blasis Amman sent at least 42 emails containing confidential information to her personal account and copied 600 files to a USB drive before her departure, which was a violation of the company's "Acceptable Use of Information Systems Policy."

These emails contained documents purportedly including some of the company's most sensitive information about its product launches and strategic planning. "The information and documents misappropriated by Amman provide a detailed roadmap to Pfizer's goals and how Pfizer specifically expects to implement these goals, both in the near term (i.e., the next 12 months) and the long term (i.e., the next 3-5 years)," the company said

The company said this position gave her access to sensitive data about the indications and treatment of patients with the condition. She also led the company's strategic planning over the marketing of the drug, giving her access to budgets, earnings and market research.

"Amman's refusal to inform Pfizer whether she planned to work for a competitor after her employment with Pfizer ended leads Pfizer to reasonably believe that she intends to provide Pfizer's confidential information to a competitor," the company said in its complaint.

According to the complaint, Amman began working for Pfizer in 2006 and rose to the position of global marketing director at the company's Collegeville, Pennsylvania, office. She was responsible for marketing the rheumatoid arthritis medication Xeljanz.

Source:

https://www.law360.com/articles/896706/pfizer-sues-ex-marketing-director-over-trade-secret-theft

Controller Accused Of Embezzling $18 Million Over 6 Years - January 23, 2017

NCI Inc. has accused its controller of embezzling approximately $18 million over the last six years and has fired him. The controller, who remained unnamed in the press release, was said to have acted alone, and NCI has launched an internal investigation with the help of outside counsel and forensic accountants.

The controller allegedly embezzled $5 million in 2016 and $13 million over the prior five years, and these amounts of money were reflected as expenses in the company's financial statements.

NCI's stock plunged Monday, dropping 9.68 percent to $12.60.
Source

Zynga Accuses Former Employees Of Trade Secret Theft - November 30, 2016

Zynga Inc. accused two former high-level workers and their new employer of stealing confidential data from the online social game maker in a lawsuit filed in California federal court.

The complaint accuses Massimo Maietti, a former senior-level game designer working on the in-development "Project Mars," and Ehud Barlach, who was a general manager of a game called "Hit It Rich! Slots," of breaching contractual obligations with Zynga over confidential information. The pair downloaded Zynga files and put them on flash drives before their last days with the company and solicited away other employees, the complaint alleges.

Both Maietti and Barlach now work for rival Scopely Inc., which is named as a co-defendant.

The complaint alleges violations of the Defend Trade Secrets Act against Scopely and Maietti, breach of contract claims against Maietti and Barlach and tortious interference with contract against Scopely.

Maietti signed an offer letter with Scopely in July, the complaint says. Though Maietti had a contractual obligation over confidential information, Zynga accuses him of using his work-issued computer to download files that "he had permission to access, but only as necessary to perform his duties for Zynga," and then copied to a USB device, according to the complaint.

"An analysis of the corresponding Google Drive folders reveals that Maietti took over 14,000 files and approximately 26 GB of extremely sensitive, highly confidential Zynga information," the complaint says.

Zynga says that Maietti took the files one day before he gave his resignation. The company says he took a folder that contained the Project Mars work, unreleased game designs, numerous documents about game play tests and financial information.
Source:
https://www.law360.com/articles/867014/zynga-accuses-former-employees-of-trade-secret-theft

Tesla Sues Former Employee For Stealing 'Hundreds Of Gigabytes' of Data - January 27, 2017
Tesla is suing an ex-employee and his business partner for breach of contract. According to the suit, former Autopilot program manager Sterling Anderson violated contractual and other obligations on his quest to launch a competing venture.

Anderson allegedly attempted to "recruit at least a dozen Tesla engineers," took "confidential and proprietary information," and doctored and destroyed evidence "in an effort to cover his tracks" on the way to founding self-driving car start-up Aurora.

In partnership with Christopher Urmson, recently departed head of Google's self-driving car initiative, Anderson used his Tesla laptop to download "hundreds of gigabytes" of confidential and proprietary information to a personal hard drive.

The luxury automaker got hip to his scheme, though, and terminated Anderson on Jan. 4—the same day he reportedly altered and wiped evidence from his company-issued laptop and smartphone, "all in an attempt to conceal his misdeeds," Tesla said.
Source:
http://www.pcmag.com/news/351365/tesla-sues-former-employee-for-stealing-hundreds-of-gigabyt

Zillow To Pay $130M To Settle Lawsuit With Move Over Alleged Trade Secret Theft - June 6, 2016
According to a Securities and Exchange Commission filing, Zillow will pay Move, which operates Realtor.com for the National Association of Realtors and owned by News Corp, a total of $130 million to settle allegations that Errol Samuelson, who was once Move's chief strategy officer, stole trade secrets and proprietary information from Move before joining Zillow in 2013.

The original lawsuit alleged breach of contract, breach of fiduciary duty and misappropriation of trade secrets and accused Samuelson of misappropriating trade secret information by acquiring it using improper means, and by copying it without authorization.
Source:
http://www.housingwire.com/articles/37204-zillow-to-pay-130m-to-settle-lawsuit-with-move-over-alleged-trade-secret-theft

Electrical Engineer For Avionics Company Convicted For Distributing Company Trade Secrets - January 6, 2016

A former electrical engineer for Pasadena-based avionics company Rogerson Kratos (RK) Avionics was convicted for distributing company trade secrets after his termination for poor performance. Using a false name and a Starbucks Internet connection, the former employee sent stolen trade secrets to other avionics companies, including one outside the United States. He was stopped when the competitors reported the economic espionage, and now faces up to 320 years in federal prison.

According to Judge Snyder's ruling, Sing's "performance at RK was marked by delays in completing assignments, late attendance and an unprofessional attitude."

Source:

http://www.justice.gov/usao-cdca/pr/glendale-man-found-guilty-32-counts-stealing-and-distributing-avionics-trade-secrets

Former U.S. State Department Employee Convicted In $2 Million Government Contract Conspiracy - July 21, 2016

Kenneth Apple, a former State Department employee, was convicted of conspiracy, wire fraud, obstruction of an official proceeding, and making false statements in connection with his role in awarding $2 million in micro-dairy contracts in Iraq to a company in which his son, Jonathan Apple, owned a 50 percent interest. Apple passed non-public information to his son, including templates and technical specifications that Jonathan Apple later used in the proposal he and his partner submitted to the U.S. Government. Apple concealed material details about the scheme, and made false statements to Federal law enforcement agents. This was a joint investigation with the FBI and the U.S. Army Criminal Investigation Command.

Source:

http://www.dodig.mil/IGInformation/IGInformationReleases/Former_U.S._State_Department_Employee_Convicted_in_2_Million_Government_Contract_Conspiracy_072516.pdf

Border Patrol Agent Charged With Bribery For Running Drugs - December 15, 2016

A U.S. Border Patrol agent in San Diego was charged Thursday with bribery for allegedly accepting $10,000 to deliver backpacks of what he believed to be smuggled methamphetamine and cocaine that were dropped along the border fence with Mexico.

The Border Patrol said Lopez has been put on unpaid leave pending the outcome of the case. He is also charged with drug-related crimes.

Lopez joined the agency 10 years ago, shortly before a massive hiring spree led to a big spike in the number of agents charged with corruption.

According to a probable cause statement, Lopez met the confidential government source in October and described how he could pick up backpacks of smuggled drugs while on patrol. He was assigned to one of the most fortified stretches of border along the U.S. divide with Mexico.

Source:

http://wtop.com/government/2016/12/border-patrol-agent-charged-with-bribery-for-running-drugs

Federal Trade Commission (FTC) Says Western Union Was Complicit In Scams - January 19, 2017

Western Union agreed to pay $586 million to settle FTC and Department of Justice charges that the company allowed scammers to use its money transfer system to collect money from their victims. The FTC says that the company's failures – **including not taking effective action against complicit agents** – resulted in hundreds of millions in fraudulent transfers since 2004. As part of this global settlement, the FTC also requires Western Union to implement an effective anti-fraud program. The Department of Justice and the FTC will use the $586 million payment to redress defrauded consumers.

Source:

https://www.ftc.gov/news-events/press-releases/2017/01/western-union-admits-anti-money-laundering-violations-settles

Former Marine Corps Contracting Officer Sentenced To 37 Months For Conspiracy - May 4, 2016,

A former Marine Corps Capt. David G. Liu was sentenced to 37 months in prison followed by 3 years of supervised release for conspiring to violate the Procurement Integrity Act. Liu was a contracting officer at the Combined Joint Task Force-Horn of Africa, Djibouti, Africa, who used his position for personal gain. From September 2012 through January 2013, Liu passed protected bid information to two contractors for use in submitting successful bids on a $495,000 blanket purchase agreement for multimedia services in Somalia. In exchange, the co-conspirators assisted Liu in paying down a debt he owed on an unrelated and unauthorized "side deal" for two government vehicles through the creation of a false government contract worth $28,000 that Liu awarded to a co-conspirator. Funds from the false contract were diverted back to Liu through a complex series of international wires and withdrawals. On February 23, 2016, co-conspirator Monroe Allen Stueber, Jr. pleaded guilty to unlawfully obtaining procurement information and was sentenced to 3 years of probation. This was a joint investigation with the Naval Criminal Investigative Service and the FBI.

Source:

http://www.dodig.mil/IGInformation/IGInformationReleases/LiuSentencingPR_050416.pdf

Peregrine Financial Group Founder Sentenced To 50 Years In Prison For Stealing $215 Million From Investors Over 20 Years - January 31, 2013

A judge sentenced Peregrine Financial Group Inc. founder Russ Wasendorf Sr. to 50 years in prison on Thursday for stealing $215 million from investors over 20 years in what a prosecutor called the biggest fraud in Iowa history.

U.S. District Judge Linda Reade told Wasendorf, 64, that the stiff sentence was warranted because of the "staggering losses" his greed caused to more than 13,000 investors, employees and creditors over 20 years. Source

Virginia Businessman Sentenced To 88 Months In Prison For Role In Bribery Scheme Involving Government Contract - October 8, 2015

Young Cho, also known as Alex Cho, chief technology officer for Nova Datacom, LLC, was sentenced to 88 months in prison and three years supervised release for a bribery scheme in which he paid millions of dollars in bribes to officials from the U.S. Army Corps of Engineers (USACE) in return for government contracts.

In addition to Cho, 19 other individuals and Nova Datacom have pleaded guilty to federal charges related to this bribery scheme.

Cho was also ordered to pay restitution of $7,656,073 to USACE and to pay a forfeiture money judgment of $6,884,948.

Source:

http://www.dodig.mil/pubs/info_detail.cfm?id=6649

Two Contractors And One Former Civilian Employee Sentenced In Bribery Scheme At Georgia Military Base - September 10, 2015

Shawn McCarty, a former civilian employee of the Marine Corps Logistics Base (MCLB), Georgia; Bradford Newell, a former MCLB contractor; and Christopher Whitman, co-owner of United Logistics (UL), were sentenced for their roles in a bribery and fraud scheme.

From 2002 through 2008, Whitman / UL paid more than $800,000 in bribes to obtain commercial trucking business from the base and approximately $200,000 for help in stealing more than $1 million in surplus Government equipment. This scheme resulted in Government losses and improper benefits to Whitman of more than $20 million.

McCarty, Newell, and Whitman were sentenced to 22, 10, and 5 year prison terms, respectively, and were ordered to forfeit assets totaling more than $34 million.

Source:

http://www.dodig.mil/IGInformation/IGInformationReleases/TwoContractorsAndOneFormerCivilian_091015.pdf

Former Security Director For Lottery Charged With Tampering Equipment Before Secretly Buying $14.3 Million Winning Ticket - April 14, 2015

If someone hasn't already sold the movie rights to the story of Eddie Raymond Tipton, expect it to happen soon. Tipton, an Iowa-based former "security director" for the Multi-State Lottery Association (MUSL), is accused of trying to pull off the perfect plot to allow himself to win the lottery. It didn't work, but not for the lack of effort. MUSL runs a bunch of the big name lotteries in the US, including Mega Millions and Powerball. It also runs the somewhat smaller Hot Lotto offering, which was what Tipton apparently targeted. When he was arrested back in January, the claims were that it had to do with him just playing and winning the lottery and then trying to hide the winnings. Lottery employees are (for obvious reasons) not allowed to play. However, late last week, prosecutors in Iowa revealed that it was now accusing Tipton of not just that, but also tampering with the lottery equipment right before supposedly winning $14.3 million.

Because of these new revelations, Tipton's trial has been pushed back until July. However, the details of the plot and how it unraveled feel like they come straight out of a Hollywood plot.

Source:

https://www.techdirt.com/articles/20150414/06370530650/former-security-director-lottery-charged-with-tampering-equipment-before-secretly-buying-143-million-winning-ticket.shtml

UPDATE:

Investigators are now looking at payouts in 37 other states and U.S. territories that used random-number generators from the Iowa-based association, which administers games and distributes prizes for the lottery consortium. Investigators have asked states to review jackpots produced by the number-generators Tipton had access to, and whose winning numbers were specifically requested by the ticket buyer. They hope to talk with anyone aware of such payouts being collected by someone other than the person who ends up with the money, said Rob Sand, a state prosecutor in Des Moines who is leading the probe.

Source:

Video:

http://launch.newsinc.com/share.html?trackingGroup=90003&siteSection=seattlepi_nws_us_sty_vmpp&videoId=29805103

News Article

http://m.seattlepi.com/news/us/article/Jackpot-fixing-investigation-expands-to-more-6707355.php

Former Intelligence Agency Official Pleads Guilty To Lying To Federal Agents About Ownership Of Private Company - August 7, 2015

Brian P. Hearing, a former official with the National Geospatial-Intelligence Agency (NGA), pleaded guilty to lying to federal investigators to conceal his ownership of a private company he was using his official position to promote.

Hearing also co-founded a private company for the purpose of developing and commercializing a certain type of automated detection system. When questioned by federal agents about his involvement with the company, Hearing lied to conceal his conflict of interest and falsely claimed that another individual was the only founder of the company. Hearing denied having any legal or financial connections to the company when, in fact, he co-founded the company and shared equal ownership of it.

Hearing worked at NGA from 2011 to 2015 in the Innovision Directorate, an applied science and technology research group. During this time,

Source:

http://www.dodig.mil/IGInformation/IGInformationReleases/HearingPR_080715.pdf

DEA Agents Get Jail Time For Running Secret Strip Club On Taxpayers' Dime - June 19, 2016

Two Drug Enforcement Administration (DEA) employees hid a strip club they owned and operated on government time from federal officials, according to court documents.

DEA workers Glen Glover of New Jersey and David Polos of New York were convicted Thursday of failing to disclose their business interests in South Hackensack, New Jersey's "Twins Plus Lounge" and conspiring to hide the club to keep their jobs and top-secret security clearances, according to the Department of Justice.

Polos was also convicted of failing to report his romantic relationship with a Brazilian dancer on federal forms when asked to disclose any close relationships with foreign nationals, the court documents show. The two purchased the club in 2010.

Source:

http://dailycaller.com/2016/06/10/dea-agents-ran-secret-strip-club-on-taxpayers-dime/#ixzz4ImWSytOB

And Many More.....

The Damages Being Caused By Insiders Are Endless.....

Investigator Discusses Navy Yard Findings, Insider Threat

3 weeks ago
www.defense.gov

97% of U.S. Enterprises Fear Insider Security Threats

Dan KobialkaVormetric, an enterprise data security solutions provider, last week released its latest Insider Threat report of big data, cloud and IT security threats.

2 weeks ago
mspmentor.net

Biggest source of DOD's cyber threats: inept co-workers

2 weeks ago
defensesystems.com

INSA Publishes White Paper on Insider Threat Programs in the US

The Cyber Council Insider Threat Task Force of the Intelligence and National Security Alliance (INSA) has published a white paper called "A Prel.....

3 months ago
news.softpedia.com

Unintentional Insider Threats: A Foundational Study

SEI Insider Threat Team, CERT. Unintentional Insider Threats: A Foundational Study (CMU/SEI-2013-TN-022). Software Engineering Institute, Carnegie Mellon University,

3 months ago
resources.sei.cmu.edu

Half of IT Decision-Makers Admit They're Vulnerable to Insider Threats

3 months ago
www.esecurityplanet.com

3 months ago
www.darkreading.com

The Enemy Within: an emerging threat...

true...

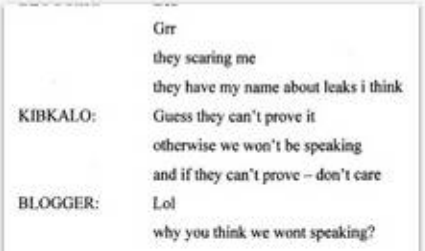
2 months ago
www.clearswift.com

US Navy Bribery Scandal: The Fourth Officer's 'Bucket List' in Exchange for Classified

5 minutes ago
www.ntd.tv

Ex-Microsoft Employee Charged With Trade Secret Theft

1 month ago
www.bloomberg.com


Grr
they scaring me
they have my name about leaks i think
KIBKALO: Guess they can't prove it
otherwise we won't be speaking
and if they can't prove – don't care
BLOGGER: Lol
why you think we wont speaking?

How Microsoft tracked down a spy who leaked its secrets

4 weeks ago
www.zdnet.com

Edward Snowden: the whistleblower behind the NSA surveillance revelations

2 months ago
www.theguardian.com

NSA employee implicated in Snowden probe resigned, memo says

2 months ago
www.washingtonpost.com

Rules that keep feds from trolling Facebook, Twitter could have led to Snowden, Alexis

1 month ago
p.washingtontimes.com

Report: Secret budget cited 4,000 NSA leaks

2 months ago
www.cbsnews.com

Ex-State Department adviser Stephen J. Kim sentenced in leak case

A former State Department arms expert who leaked classified information to a Fox News reporter was sentenced Wednesday to 13 months in prison after a pointed court-

3 weeks ago
www.washingtonpost.com

Hundreds of Classified Leaks Under Review by IC Inspector General

Hundreds of cases of unauthorized disclosures of classified information were under review by the Office of the Inspector General of the U.S. Intelligence Community

2 months ago
blogs.fas.org

APNewsBreak: Defense contractor to plead guilty

1 month ago
www.federalnewsradio.com

Engineer accused of trying to smuggle military jet engine documents, blueprints to Iran

3 months ago
www.foxnews.com

Army Officer Freaks Out Thousands Of Government Employees With Cybersecurity

1 month ago
www.businessinsider.com

Stolen F-35 secrets now showing up in China's stealth fighter

1 month ago
www.foxnews.com

Hawaii soldier accused of spying convicted

2 months ago
www.hawaiinewsnow.com

Navy Suspends Admirals' Access to Classified Information

The U.S. Navy suspended access to classified information for two of its top admirals handling intelligence matters after putting them on leave this week pending a review of

3 months ago
www.bloomberg.com

Naval Espionage: Stopping a Dangerous Insider Threat

1 month ago
www.fbi.gov

U.S. Marine Pleads Guilty in Identity Theft Tax Refund Fraud Scheme Targeting U.S. Marines

2 months ago
www.fbi.gov

Former defense contractor pleads guilty to sharing classified documents

Federal prosecutors say 50-year-old Bruce Schliemann, a former defense contractor and retired Navy SEAL, faces up to one year in prison and/or a fine of up to $100,000 when

3 months ago
www.federalnewsradio.com

WASHINGTON: 'Zero Dark Thirty' leak investigators now target of leak probe | Insider

2 months ago
www.mcclatchydc.com

IRS Financial Systems Vulnerable to Insider Threats

2 months ago
www.govinfosecurity.com

Congress Presses TSA To Crack Down On "Insider Threats" From It's Own Employees

2 months ago
www.prisonplanet.com

LewisGale Regional Health System Suffers Insider Breach

2 weeks ago
www.esecurityplanet.com

Arcadia Home Care Acknowledges Insider Breach

1 month ago
www.esecurityplanet.com

Leader of ID Theft Ring Targeting Government Employees Sentenced to 12

1 month ago
news.softpedia.com

IRS Employee Takes Home Thumb Drive With Data on 20,000 Colleagues

1 month ago
www.nextgov.com

Fort Benning Employee Charged with $2.2 Million Identity Theft Scheme Targeting

Tracy Mitchell allegedly used service members' stolen identities to file more than 1,000 fraudulent tax returns....

2 months ago
www.esecurityplanet.com

Miami Police Officer Gets 12 Years in Prison for Identity Theft

Malinsky Bazile used Florida's driver's license database to steal the identities of 700 middle-aged women....

2 months ago
www.esecurityplanet.com

Two Men Jailed for Identity Theft at Medical Lab

Angelo Ponds and Sean Guillaume were sentenced to 48 months and 94 months in prison, respectively....

2 months ago
www.esecurityplanet.com

Home Depot Employees Arrested for Insider Breach

2 months ago
www.esecurityplanet.com

Insider suspected of stealing payroll data on 100K Morrisons staffers

1 month ago
www.scmagazine.com

Former Mount Sinai Medical Center Employee Jailed for Identity Theft

Oliver Gayle was sentenced to 51 months in prison....

2 months ago
www.esecurityplanet.com

Former TD Bank Employee Admits Identity Theft

1 month ago
www.esecurityplanet.com

North Country Hospital Acknowledges Another Data Breach

2 months ago
www.esecurityplanet.com

Two Sentenced for Identity Theft Scheme Targeting U.S. Government Employees

3 months ago
www.esecurityplanet.com

Log audit reveals developer outsourced his job to China

3 months ago
www.net-security.org

Feds: Ex-Lilly employees sold secrets

3 months ago
www.theindychannel.com

Veterans' Hospital Volunteer Charged with Theft of Patients' Identities

Ricardo Jacinto Rodriguez is accused of stealing 106 patients' names and Social Security numbers, which were then used to file fraudulent tax returns....

3 months ago
www.esecurityplanet.com

Prison Medical Records Clerk Indicted for Identity Theft

3 months ago
www.esecurityplanet.com

State Farm Admits Insider Data Breach

A call center employee misused at least 11 customers' credit card numbers....

3 months ago
www.esecurityplanet.com

Holy Cross Hospital Acknowledges Insider Breach

Patients' names, birthdates, addresses and Social Security numbers were accessed by a former employee....

3 months ago
www.esecurityplanet.com

California's Northern Inyo Hospital Suffers Insider Data Breach

'A hospital can only do so much in the case of a rogue employee,' hospital administrator John Halfen said....

3 months ago
www.esecurityplanet.com

Bed Bath and Beyond Acknowledges Insider Breach

A cashier stole an undisclosed number of customers' credit card information....

3 months ago
www.esecurityplanet.com

HSBC Acknowledges Insider Breach

3 months ago
www.esecurityplanet.com

UConn Health Center Admits Second Insider Breach This Year

3 months ago
www.esecurityplanet.com

W.J. Bradley Mortgage Capital Admits Insider Breach

3 months ago
www.esecurityplanet.com

Washington Court Clerk Fired for Insider Breach

3 months ago
www.esecurityplanet.com

Riverside Health System Acknowledges Four-Year Insider Breach

3 months ago
www.esecurityplanet.com

Systems Administrator Admits Sabotaging Ex-Employer's Server

3 months ago
www.esecurityplanet.com

The [National Insider Threat Special Interest Group](https://flipboard.com/@cybercops911/nitsig-insider-threat-awareness-resource-guide-tkh6a9b1y) **keeps and updated list of "Insider Threat Incidents"**

https://flipboard.com/@cybercops911/nitsig-insider-threat-awareness-resource-guide-tkh6a9b1y

Reports And Surveys Show A Continued Problem With The Insider Threat

Association Of Computer Fraud Examiners Fraud Report - 2016

Highlights

- The total loss caused by the cases in our study exceeded $6.3 billion, with an average loss per case of $2.7 million.
- Fraud perpetrators tended to display behavioral warning signs when they were engaged in their crimes. The most common red flags were living beyond means, financial difficulties, unusually close association with a vendor or customer, excessive control issues, a general "wheeler-dealer" attitude involving unscrupulous behavior, and recent divorce or family problems. At least one of these red flags was exhibited during the fraud in 78.9% of cases.
- The most prominent organizational weakness that contributed to the frauds in our study was a lack of internal controls, which was cited in 29.3% of cases, followed by an override of existing internal controls, which contributed to just over 20% of cases.
- The more individuals involved in an occupational fraud scheme, the higher losses tended to be. The median loss caused by a single perpetrator was $85,000. When two people conspired, the median loss was $150,000; three conspirators caused $220,000 in losses; four caused $294,000; and for schemes with five or more perpetrators, the median loss was $633,000.
- More occupational frauds originated in the accounting department (16.6%) than in any other business unit. Of the frauds we analyzed, more than three-fourths were committed by individuals working in seven key departments: accounting, operations, sales, executive/upper management, customer service, purchasing, and finance.
- In cases detected by tip at organizations with formal fraud reporting mechanisms, telephone hotlines were the most commonly used method (39.5%). However, tips submitted via email (34.1%) and web-based or online form (23.5%) combined to make reporting more common through the Internet than by telephone.

Summary

http://www.acfe.com/rttn2016/about/executive-summary.aspx

Full Report

https://s3-us-west-2.amazonaws.com/acfepublic/2016-report-to-the-nations.pdf

Healthcare Data Breaches Report - January 19, 2017

Highlights

- Data breaches in the U.S. healthcare field cost $6.2 Billion dollars each year.
- The average cost of a single data breach across all industries is $4 Million dollars, according to a 2016 study from IBM and Ponemon Institute.
- Approximately 90% of hospitals have reported a breach in the past two years, and most breaches are due to employee error.
- The average HIPAA settlement fine is approximately $1.1 Million dollars.
- Data Breach notification costs $560,000 on average
- Costs affiliated with lawsuits average $880,000.00.
- Post data breach cleanup costs average $440,000.00
- Healthcare organizations average $500,000.00 in lost brand value after a data breach, with some estimates reaching $50 Million dollars as an average amount in lost brand value.

Source:

http://www.beckershospitalreview.com/healthcare-information-technology/healthcare-breaches-cost-6-2b-annually.html

Verizon 2016 Data Breach Investigations Report (DBIR) - Humans Remain The Weakest Link

According to the report authors, cyber criminals are continuing to exploit human nature as they rely on familiar attack patterns such as phishing. However, 'Miscellaneous errors' by end users of an organization took the top spot for security incidents in this year's report.

“These can include improper disposal of company information, mis-configuration of IT systems, and lost and stolen assets such as laptops and smartphones,” Verizon said. The report found that 26% of these errors involved people mistakenly sending sensitive information to the wrong person. "You might say our findings boil down to one common theme -- the human element," said Bryan Sartin, executive director of global security services, Verizon Enterprise Solutions. "Despite advances in information security research and cyber detection solutions and tools, we continue to see many of the same errors we've known about for more than a decade now. How do you reconcile that?"

Contrary to what some people think, it’s rarely system administrators or developers with elevated privileges that fall victim. End users account for a third of insider misuse. Attacks are typically motivated by money: 34% of breaches involving misuse were motivated by financial gain—although a quarter (25%) can be linked with espionage, such as the theft of intellectual property.

Only a small percentage (14%) are in leadership roles (executive or other management), or in roles with elevated access privilege jobs such as system administrators or developers (14%). The moral of the story is to worry less about job titles and more about the level of access that every Joe or Jane has (and your ability to monitor them).

Source:

http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Department Of Justice Task Force On Intellectual Property - June 2, 2016

In the U.S. alone, trade secret theft costs innovators an estimated $450 billion per year and constitutes a threat to U.S. security and the U.S. economy. Thanks to increasing employee mobility, data transfer capabilities, and globalization, trade secret loss is a growing threat to innovators worldwide. U.S. courts have recognized the great value of trade secrets. For example, in 2011, a California court awarded a global medical device company $2.3 billion for trade secret theft by a former employee. Beyond economic value, trade secret misappropriation is also a threat to safety and security—multiple former employees of defense contractors have been caught attempting to sneak valuable military secrets to both Iran and China.

The importance of trade secret protection cannot be overstated. And the threat is often closer than you think. In a recent Symantec study, 50 percent of employees surveyed who left or lost their jobs said that they retained confidential corporate data, and 40 percent planned to use that data in their new jobs. Further, 62 percent believe it is acceptable to transfer work documents to personal devices or online sharing applications, and generally fail to delete the data afterwards.

A 2015 Ernest & Young Global Information Security Survey found that 88 percent of corporate counsel said that the current security measures at their company are insufficient to prevent trade secret misappropriation. In this study, corporate counsel saw employees as the second-largest threat to trade secret security, behind only criminal syndicates.

Source:

http://globalcompliancenews.com/trade-secrets-20160602/

FBI / Department of Homeland Security

- A recent (2014) FBI and Department of Homeland Security alert reported that employees with an ax to grind are increasingly using Internet cloud services and other computer tools to hack their current or former companies.
- Companies victimized by current or former employees incur costs from $5,000 to $3 million.
- According to the FBI our nation's secrets are in jeopardy, the same secrets that make a company profitable. The FBI estimates billions of U.S. dollars are lost to foreign competitors every year. These foreign competitors deliberately target economic intelligence in advanced technologies and flourishing U.S. industries. External data breaches by cyber criminals get a lot of attention, but frequently insiders are recruited by foreign competitors to gather and steal a company's data.

Verizon Data Breach Report (2015) (Source)

- As with prior years, 55% of incidents were privilege abuse—which is the defining characteristic of the internal actor breach. Insiders abusing the access they have been entrusted with by their organization, was in virtually every industry.
- Financial gain and convenience were the primary motivators in 40% of incidents, whether the insider planned to monetize stolen data by selling it to others (such as with financial data), or by directly competing with their former employer.

Insider Threats To Credit Unions (2015) (Source)

- 83% of surveyed financial institutions admit their biggest con
- cern is confidential information transferred to unauthorized recipients.
- 52% say they are worried about sensitive data being transferred by use of removable media.
- 77% of all credit unions surveyed said they do not believe or were unsure if they had complete protection regarding internal data threats.
- 62% stated they already have security controls in place.

Insider Threats To Healthcare (2015) (Source)**:**

- 92% of 102 U.S.-based healthcare IT decision makers surveyed said their organizations are either "somewhat" or more vulnerable to insider threats.
- 49% felt "very" or "extremely" vulnerable to insider threats.
- 48% of healthcare organizations experienced a data breach or failed a compliance audit in the past year.
- 63% of healthcare IT decision makers said their organizations are planning to increase spending to offset data threats.

SANS / Spectorsoft Survey (2014, 2015) (Source)

- 74% of the 772 IT security professionals surveyed said they're concerned about insider threats from negligent or malicious employees.
- 32% said they have no ability to prevent an insider breach.
- 28% said insider threat detection and prevention isn't a priority in their organizations.
- 44% of respondents said they don't know how much they currently spend on solutions to mitigate insider threats.
- 45% said they don't know how much they plan to spend on such solutions in the next 12 months.
- 69%of respondents said they currently have an incident response plan in place, but more than half of those respondents said that plan has no special provisions for insider threats.
- 52% of survey respondents said they didn't know what their losses might amount to in the case of an insider breach.

The 2015 SolarWinds Survey Investigates Insider Threats to Federal Cybersecurity (Source)

- More than half (53%) of federal IT Pros identified careless and untrained insiders as the greatest source of IT security threats at their agencies, up from 42 percent last year.
- Nearly two-thirds (64%) believe malicious insider threats to be as damaging as or more damaging than malicious external threats, such as terrorist attacks or hacks by foreign governments.
- Further, 57% believe breaches caused by accidental or careless insiders to be as damaging as or more damaging than those caused by malicious insiders.
- Nearly half of respondents said government data is most at risk of breach from employees' or contractors' desktops or laptops. Top causes of accidental insider breaches include phishing attacks (49%), data copied to insecure devices (44%), accidental deletion or modification of critical data (41%) and use of prohibited personal devices (37%).

The 2015 Vormetric Insider Threat Report (Source) (Video)

- 93% of U.S. respondents said their organizations were somewhat or more vulnerable to insider threats.
- 59% of U.S. respondents believe privileged users pose the biggest threat to their organization.
- Preventing a data breach is the highest or second highest priority for IT security spending for 54% of respondents' organizations.
- 46% of U.S. respondents believe cloud environments are at the greatest risk for loss of sensitive data in their organization, yet 47% believe databases have the greatest amount of sensitive data at risk.
- 44% of U.S. respondents say their organization had experienced a data breach or failed a compliance audit in the last year.
- 34% of U.S. respondents say their organizations are protecting sensitive data because of a breach at a partner or a competitor.

The 2014 U.S. State Of Cyber Crime Survey (Source)

- The incidents that typically fly under the media radar are insider events.
- 28% of respondents pointed the finger at insiders, which includes trusted parties such as current and former employees, service providers, and contractors.
- 32% say insider crimes are more costly or damaging than incidents perpetrated by outsiders. The larger the business, the more likely it is to consider insiders a threat; larger businesses also are more likely to recognize that insider incidents can be more costly and damaging.
- Only 49% of all respondents have a plan for responding to insider threats.

The 2014 Occupational Fraud And Abuse Report By The Association Of Certified Fraud Examiners (ACFE) (Source)

- Companies lose 5 percent of revenue each year to fraud, which amounts to nearly $3.7 trillion globally.
- The report pegged the median loss from fraud at $145,000. More than 1 in 5 of the almost 1,500 cases analyzed in more than 100 countries had employees walking away with at least $1 million.

GAO Report On Personnel Security Clearances

- A 2014 Government Accountability Office (GAO) report reviewed the eligibility of individuals accessing classified information.
- Access to classified information was revoked in 2009-2013 for more than 18,500 military and civilian employees and contractors working for the Department of Defense (DoD), according to an audit. (16,000 Military-Civilian Employees And For 2,500 contractors).
- The report examined the most common reasons for revoking clearances by the DoD for fiscal year 2013. The top causes for civilian and military personnel were criminal conduct, involvement with drugs and personal conduct. Top reasons for contractors were financial considerations and personal and criminal conduct.
- The report also examined revocations by the Department of Homeland Security (DHS), although only for fiscal year 2013. About 125,000 DHS civilian and military employees were eligible to access classified information as of March 2014. DHS revoked eligibility for 113 personnel during fiscal year 2013 the report said.

Organizations Lack Training And Budget To Mitigate Insider Threats

- **A** 2014 Insider Threat Survey conducted by Spectorsoft of 355 IT and security professionals revealed the following;
  - 61% stated they didn't have the ability to deter an insider threat.
  - 59% stated they couldn't detect an insider threat.
  - 60% of stated that they weren't prepared to respond to insider attacks.
  - 35% stated that they had already experienced an insider attack, with 41% of those attacks involving financial fraud, 49% of them involving a data leak, 16% involving intellectual property theft.

Additional Insider Threat Reports

- GAO Report: Insider Threats In The DoD (2015)
- DHS Report On Insider Threat Problems At U.S. Coast Guard (2015)
- Carnegie Mellon University CERT Insider Threat Center Reports / Publications
- 2014 Vormetric Insider Threat Report (2014)
- GAO Report - Additional Guidance And Oversight Needed At DHS And DOD To Ensure Consistent Application Of Revocation Process (2014)
- A Worst Practices Guide To Insider Threats: Lessons From Past Mistakes (2014)
- U.S. State Of Cyber Crime Survey (2013)
- Secretary Of Defense Recommendations On Washington Navy Yard Shootings (3-2014)
- DHS Report - Risks To US Critical Infrastructure From Insider Threat (12-2013)
- DoD Internal Review Of Washington Navy Yard Shooting (2013)
- RSA 2014 Conference Presentation On Insider Threats - INSA Insider Threat Report
- INSA Report: Preliminary Examination Of Insider Threat Programs In The U.S. Private Sector (2013)
- Vormetric-Insider Threat Research Survey (2013)
- Vormetric Insider Threat Report - Financial Services (2013)
- DHS OIG Report US CBP Regarding Insider Threat Program (9-2013)
- DHS OIG Report On TSA Insider Threat Problem (9-2012)
- GAO Report - IRS Needs To Enhance Internal Control Over Financial Reporting And Taxpayer Data (3-2011)
- DHS OIG Report Examining Insider Threat Risk At The U.S. Citizenship And Immigration Services (1-2011)
- Insider Threat To Critical Infrastructure Study - Final Report And Recommendations (2008)
- DoD PERSEREC: Espionage By Americans From 1947-2007
- DoD PERSEREC: Espionage Case Summaries From 1975-2008
- DoD Insider Threat Mitigation Report (2000)

ABOUT THE NITSIG

The National Insider Threat Special Interest Group (NITSIG) was created to assist individuals (Nationwide) working for the; U.S. Government, State Governments, Department of Defense, Intelligence Community Agencies, Critical Infrastructure Providers, Defense Industrial Base contractors, Aviation / Airline Industry, Technology Companies, Banking - Financial Industry, large and small businesses and others with a **central source** for Insider Threat Security, Education, Training and Awareness.

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

- ✓ Insider Threat Program Development, Implementation & Management
- ✓ Insider Threat Program Working Group / Hub Operation
- ✓ Insider Threat Awareness and Training
- ✓ Insider Threat Risk Mitigation (Assessments & Mitigation Strategies)
- ✓ User Activity Monitoring / Behavioral Analytics Tools
- ✓ Workplace Violence Guidance / Active Shooter Response Guidance & Training

NITSIG Membership Overview And Application

The NITSIG Membership is **FREE**. To join the NITSIG you must complete and sign the NITSIG Membership Application. Instructions for sending the membership application to the NITSIG are in the application. You will be put on the NITSIG e-mail distribution list for future NITSIG meeting announcements and other relevant information. NITSIG Members will receive a monthly Cyber Security-Insider Threat News E-Magazine.
www.nationalinsiderthreatsig.org/nitsigmembership.html

NITSIG Meetings

The NITSIG has monthly meetings primarily held at the John Hopkins University Applied Physics Lab in Laurel, Maryland. There is NO CHARGE to attend. Other NITSIG meetings maybe held at other NITSIG Sponsor locations. See the link below for some of the great speakers we have had at NITSIG meetings:
http://www.nationalinsiderthreatsig.org/nitsigmeetings.html

ABOUT INSIDER THREAT DEFENSE

Insider Threat Defense has become the "Leader-Go To Company" for Insider Threat Program Development Training and Insider Threat Risk Management Services. We provide a broad portfolio of training and services to potential clients, that will address "Insider Threat Risks" with a cost effective, comprehensive and holistic approach.

Insider Threat Defense has a very impressive portfolio of clients and has provided our training and services to 500+ organizations; U.S. Government Agencies (Department of Defense, Intelligence Community), Defense Contractors, NCMS Members / Chapters, Defense Security Service, Critical Infrastructure Providers, Aviation / Airline Industry, Spacecraft Manufacturing-Launch Providers, Technology Companies, Banking - Financial Industry, large and small businesses.

We offer our clients proven Experience, Past Performance, Comprehensive Training, Commitment, Research, Collaboration, Awards.

Past clients are rating our Insider Threat Program Development Training and Insider Threat Risk Mitigation Services in the "Above Average" to "Excellent" Category. (References Available Upon Request) (Client Comments)

Please visit the Insider Threat Defense website for more information.

CONTACT INFORMATION

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense, Inc.
Insider Threat Program Development Training Course Instructor / Risk Mitigation Specialist
Cyber Security-Information Systems Security Program Management Training Course Instructor
Founder / Chairman Of The National Insider Threat Special Interest
FBI Maryland InfraGard Member
888-363-7241 / 561-809-6800
www.insiderthreatdefense.us
www.nispomcc2training.com
james.henderson@insiderthreatdefense.us
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org