Minimizing Insider Threat Risk with Behavioral Monitoring

I. Hilmi Elifoglu

Ivan Abel

Özlem Taşseven

Abstract

An insider is a person that has or had a legitimate right to access computing resources of an organization. This definition includes any current or former employee, contractor, customer, or business partner as an insider.

Insider threat is the potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization. Insiders may pose a greater threat to cybersecurity than all outside malicious actors combined. The average damage per insider incident is known to be much higher than the outsider attacks, in some instances causing millions of dollars of damage in the form of fraud, sabotage, and the theft of trade secrets or intellectual property. WikiLeaks' disclosures and industrial espionage cases reported by the FBI show the importance of the insider issue.

Until recently, the insider threat did not mean much to the information technology field. As trusted employees or business partners, the insiders were trusted to do what was in the best interest of an organization. Since insiders are already authenticated and inside the system, it is very difficult to pinpoint exactly at what point the insider has become an insider threat.

Contrary to the common belief, most insider incidents are not based on sophisticated hacker tools. Most insider threat incidents are the consequences of human actions, such as mistakes, negligence, greed, or reckless behavior.

Statistical and analytical prediction models and technical security tools, such as anti-virus software, firewalls, and intrusion-detection systems, have not been very successful in predicting the multi-faceted insider behavior. Because of the human factor, a multidisciplinary people-centric approach is needed.

This paper attempts to provide a checklist of best practices against the insider threat by improving the collaboration between the information technology (IT) management and the human resources (HR) department.

I. Hilmi Elifoglu, PhD, MBA, is an Associate Professor at the Peter J. Tobin College of Business, St. John's University, New York. elifogli@stjohns.edu

Ivan Abel, PhD, MBA, is an Associate Professor at the Peter J. Tobin College of Business, St. John's University, New York. abeli@stjohns.edu

Özlem Taşseven, PhD, is an Associate Professor in the Department of Economics, Doğuş University, Istanbul, Turkey. otasseven@dogus.edu.tr

INSIDERS AND THE INSIDER THREAT

What distinguishes an information system (IS) insider from an outsider is his or her current or past association with the system. This definition of an insider includes current and former employees, contractors, customers, and business partners. The term can also apply to an outside person who poses as an employee or officer by obtaining false credentials.

As a federally funded premier research and coordination center for cybersecurity issues, the CERT (Computer Emergency Response Teams) at the Software Engineering Institute of Carnegie Mellon University have recently provided an updated definition of the insider threat. The insider threat is the potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization (Costa, 2017).

The insider threat did not mean much to the computer field until recent years. Even after WikiLeaks (BBC News, 2017) and the Snowden cases (Wikipedia, n.d.), most information system budgets and resources are still aimed at the detection and prevention of attacks from external sources. The reasoning is the belief that the insiders, as trusted users, usually do what is in the best interest of the organization.

Unfortunately, whether intentional or not, all insider incidents can have devastating effects on the system.

Intentional Versus Unintentional Insider Threat

The insider threat comes from the abuse or misuse of the computer usage privileges. These privileges are summarized as read, write, and execute privileges for each user or user groups by an operating system. If the threat is intentional, it is called a *malicious attack*. If the intent to harm the organization is missing, the misuse is called *accidental*. Intentional abusers include disgruntled employees, activists, terrorists, organized crime members, competitors, thieves, and irrational individuals. The theft of intellectual property, industrial espionage, sabotage, and terrorism are typical examples of intentional abuse.

In contrast to malicious attacks, most accidental misuses take place because of inadequate training, stress, carelessness, loss of devices, desire to help others, or vulnerability to blackmail or social engineering.

The following are some of the most common insider threat incidents:

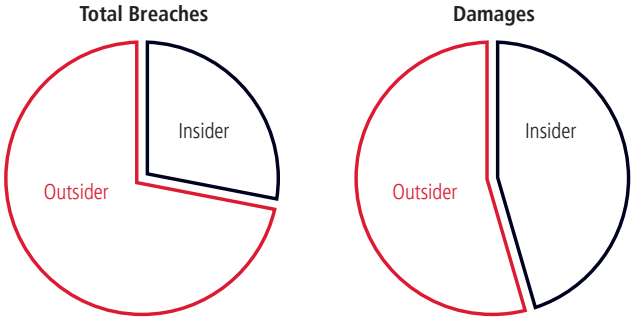
- Lost equipment, such as a laptop, tablet, or data disk with sensitive information
- Unauthorized setup of modems, or unauthorized setup of remote access programs or wireless access points
- Use of corporate computing devices for non-business purposes
- Use of personal devices for business purposes
- Use of personal email accounts for business
- Deletion of data files, or accidental disclosure of sensitive material using email or fax
- Use of business email for personal correspondence
- Non-work-related web browsing

- Downloading unauthorized software/media files from unauthorized sites and bringing in malware or spyware
- Accidental unauthorized copying of files to portable storage devices
- Instant messaging using personal accounts

Privileged User as an Insider Threat

A privileged user is a user who, by virtue of function and/or seniority, has been allocated powers within the computer system that are significantly greater than those available to the majority of users. There are few things these types of users cannot do. Equipped with powerful privileges to navigate many areas of the systems, the privileged users can access many layers of network and operating system without much difficulty, such as changes in hardware and software configurations and file systems.

FIGURE 1. An Overview of Insider Incidents and Damages



Source: SEI. 2014. U.S. State of Cybercrime Survey. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

As expected, the damage caused by privileged insiders is much higher than average insiders (Figure 1). According to a national fraud survey conducted by the Association of Certified Fraud Examiners, the cost of insider attacks to United States businesses is around $400 billion per year. Of that, $348 billion can be tied directly to privileged users, according to a CSO Online article (Lovejoy, 2006). The damage by a privileged power user, such as root or database administrator (DBA), can affect the information system as a whole.

The detection and prevention of the damage from this type of power user will be more complicated because they can bypass many of the security controls and can reach the most critical IT assets with ease. By creating fake user accounts, they can delete any trace of their actions. While conducting these activities, their actions may still look like their authorized day-to-day online activities. Therefore, detection and taking precautionary actions against the IT professional is more complicated.

Non-Employees as an Insider Threat

The insider threat is not limited to the employees of an enterprise. Many legitimate outside users, such as internet service providers, cloud service providers, telephone companies, customers, suppliers, and temporary or short-term personnel should also be considered insiders. Unless properly controlled, all of these groups have the opportunity to reach inside corporate networks and steal unprotected data.

Recent Insider Cases from the Media

Here are some recent security incidents involving various types of insiders:

- *Waymo (v. Uber) claims* an engineer downloaded thousands of files about self-driving car technology and shared with Uber before starting to work for Uber's Autonomous Driving Car Unit (Lawler, 2017).
- *A Ford employee* copied proprietary documents, including some on sensitive designs, to an external hard drive and was arrested at an airport shortly before reporting for a new job with a competing firm in China (FBI, 2011).

- *Two long-time DuPont employees (retired)* stole data for manufacturing titanium dioxide based paint (Wilber, February 4, 2016).
- *A former Fannie Mae employee* installed a logic bomb that (had it not been discovered) would have shut down the information system by decimating thousands of servers (Moscaritolo, 2009).

Other Classifications of Insiders

The success of prevention policies against the insider threat depends on the proper classification of the source. The following lists some of the classifications used by security researchers:

- Employment status of the user (e.g., employees versus business partners)
- Types of assets misuser accessed (e.g., physical versus logical)
- Saboteur or thief: This group will maliciously hack into areas of the IT system to which they shouldn't have access or infect the network purposely from within
- The security softie: This group has a very limited knowledge of security and put their business at risk through using their work computer at home or letting family members surf the Internet on their work computer
- The gadget geek: Those that come to work armed with a variety of devices/gadgets, all of which get plugged into their PC
- The squatter: Those who use the company IT resources in ways they shouldn't (e.g., by storing content or playing games) (US-CERT, n.d.)

Each of these classifications can be analyzed further in greater detail. For instance, the employment relationship may be classified further as current versus former, temporary versus permanent employees. Insiders, who do not have an employee status, can also be looked at: customers, contractors, and business partners. Similarly, the accessed assets may also be grouped as hardware, network, or data and intellectual property. The harm done may also be grouped as fraud, theft of intellectual property, cyber sabotage, and spying.

HIGHLIGHTS FROM THE U.S. CURRENT INSIDER SURVEYS

The CERT Division of the Software Engineering Institute at Carnegie Mellon University, in cooperation with the U.S. Secret Service and the FBI, conduct some of the most comprehensive cyber security surveys for the United States on an annual basis. The result of the interviews with hundreds of IT professionals are published in their websites. The following is a summary of significant findings from recent surveys on the insider threat:

- Approximately half of the organizations had some insider security incident every year between 2002 and 2014.
- In other words, the insider incidents are common occurrences (CERT 2014).

TABLE 1. Most Common Damages from the Insider Incidents

Stolen or compromised confidential information (such as trade secrets or intellectual property)	32%
Stolen or compromised customer information	33%
Stolen or compromised employee records	40%
Unintentionally exposed private or sensitive information	50%

Source: SEI. 2016. U.S. State of Cybercrime Survey. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

- Even though hacker incidents outnumber insider incidents, the insider incidents are equally dangerous. The insider incidents are costlier on a per-unit basis. The average damage was estimated to be $412,000 (Richards, 2013).
- In financial terms, the aggregate damage caused by insiders is close to the aggregate damage caused by hackers. In several instances, damages reached more than $1 billion (Richards, 2013).
- The typical insider threat is the violation of confidentiality and privacy, such as looking at payroll data. Approximately three-quarters of the insider incidents are related to revealing employee and customer records. The second most damaging common insider incident is the theft of trade secrets and intellectual property (see Table 1). One-third of the firms interviewed reported either stolen intellectual property or customer-related data.

PREDICTION AND DETECTION

Business organizations try to protect themselves by predicting the insider incidents before an incident takes place. Predicting the insider incident means predicting who will turn against his or her organization. Unfortunately, there is no single answer why some people turn against their own interests or their own organizations. Many attempts to preempt the multi-faceted insider incidents have not been successful.

There are two alternatives: technical and behavioral monitoring, or a combination of the two. Some organizations prefer technical monitoring tools, e.g., NetFlow from Cisco; others use a behavioral monitoring approach to keep an eye on the insiders (Cisco, 2018).

Technical Monitoring

Utilizing advanced monitoring software, artificial intelligence, and machine learning techniques, enterprises can analyze critical data across the entire enterprise, establish baselines of normal behavior, and identify anomalous activities and outliers.

The following is some popular technical monitoring topics against the insider threat:

- Unauthorized copying of files to portable storage devices
- Large or unusual quantities of data leaving an enterprise through email or fax
- Downloading unauthorized software, data, or media content

- Changes in data access patterns e.g., frequency, time, and location
- Failed authentication attempts
- Unusual attempts to retrieve data from backup or archive
- Changes in protocols used, unexpected or unusual command usage
- Unauthorized setup of remote access programs, modems
- Use of personal computing devices for business
- Using business computers for personal use
- Using personal email accounts for business, or using a business email account for personal correspondence
- Unexpected sharp increase in print jobs
- Unauthorized privilege escalation
- Modification or deletion of audit logs
- Unauthorized deletion or modification of data and log files
- Changes to the system infrastructure

The success of technical monitoring depends on an IT infrastructure built on the principles of *need-to-know, least privilege,* and *segregation of duties*. Based on these principles, the organization should be aware of *privilege creep*. When an employee is assigned a new role, the privileges of the previous role should be taken away after a short transition period. Each user's privileges should be reviewed at least once a year. Only the privileges directly associated with the current title and responsibilities should be given to each insider.

Behavioral Monitoring

The behavioral monitoring focuses on the insider. In contrast to common belief, the malicious insider is not a hacker equipped with special sophisticated technical tools. Most malicious insiders do not use any fancy technical tools. These are people doing authorized things with malicious intent. The traditional technical tools will fail to detect these incidents in a timely manner. The respondents of the CERT surveys usually admit that even after an incident, a large percentage of sensitive material and intellectual property (IP) thefts are discovered after notification from the FBI (Cushing, 2017).The FBI also admits the risk from the insider threat is not technical, it is people-related, suggesting a behavioral monitoring approach. Previous FBI efforts to predict the malicious behavior with statistical models and technical monitoring did not fare well. Because of complications in determining the human motives and behavior, the technical monitoring tools should be complemented with behavioral monitoring tools without violating the local regulations about privacy (Dark Reading, 2013).The discontent at the workplace seems to be one of the most significant motives for the intentional privilege misuse. Layoffs, demotions, pay cuts, delayed promotions, or other management practices deemed to be unfair, provide the necessary justification for privilege misuse by a disgruntled employee, retiree, or business partner. An employee who did not receive promotion or recognition may be tempted to misuse his or her privileges or knowledge to reach sensitive materials. Stealing and selling confidential information may be considered revenge by the disgruntled

employee. For instance, the theft of DuPont's trade secret white color, based on retiree disclosures made many years after their retirement shows how strong feelings can be (Wilber, February 4, 2016). As we have seen in the Edward Snowden case, ideological differences may also lead to revealing confidential information.

In general, any negative change in the behavior of an insider should be a concern for management. As one may notice, most of these behavioral topics are in HR territory. Below is a list of significant behavioral indicators that should be shared by the HR department:

- Sudden change in financial status: sudden wealth or sudden excessive debt
- Recent legal restraining orders
- Wage garnishments
- Alcohol, drug dependency
- Disregard for authority and accepted practices
- Attempts to circumvent security requirements
- Unusual business or personal travels
- Association with hostile groups, and social media indicators
- The degree of dissatisfaction with their work
- Mental instability
- Major life events
- Negative reviews

TABLE 2. Most Common Forms of Unintentional Insider Incidents

Social engineering	21%
Laptops	18%
Remote access	17%
E-mail	17%
Copy of data to mobile device	16%

Source: SEI. 2014. U.S. State of Cybercrime Survey. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

With accidental misusers, a desire to help others, careless or reckless use of the information system, lost equipment, and vulnerability to social engineering are some of the leading reasons. In the context of information security, social engineering is defined as tricking people into divulging confidential or personal information. According to the CERT report, 21 percent of the fraudulent attacks were initiated by social engineering or taking advantage of human nature to be helpful to a friend or colleague. Stolen or lost laptops (18 percent) as well as downloading data, media files, or software from unauthorized websites are also common causes of insider threats (Table 2).

Popular Responses to the Insider Threat

As expected, because of perceived difficulties in winning a conviction and other financial concerns, many insider incidents go unreported. To win in court, U.S. companies must prove that they properly safeguarded their trade secrets, something many fail to do. In some instances, companies worry that disclosing an industrial espionage case will hurt their stock prices, harm relationships with their customers, or prompt federal agents to put them under a microscope (Wilber, February 8, 2016). Therefore, very few cases of the insider incidents are reported. We can easily assume that the published statistics underestimate the actual numbers of the insider incidents.

The following are the statistics, derived from the CERT reports, showing how most insider attacks are handled by U.S. firms (US-CERT, n.d.).

- Approximately three-quarters of the insider incidents are handled internally without any involvement by the law-enforcement authorities. Only 10 percent of the cases were deemed to be "some kind of internal legal action." When asked about why they did not prosecute the insiders after a security breach, a third of the respondents claimed that incidents were found to be insufficient to warrant prosecution, or there was not enough evidence to identify individual(s) behind the incident. Another popular cause for handling the issue internally was the concern about the negative publicity and the competition's use of the information to their advantage.
- Overall, only 15 percent of the cases were deemed to be worthwhile to process further outside the organization. External law enforcement agencies were informed in 12 percent of the cases. In only 3 percent of the cases, there were civil proceedings against the user.
- Despite the pervasiveness and persistence of insider incidents, less than half (49 percent) of organizations reported having a formal plan for responding to insider incidents. Eleven percent of organizations did not have any response mechanism for insider security events (Table 3).

Best Practices for Deterrence

Firing an employee is one way to deal with the insider incident.

Unfortunately, as various CERT surveys over the years have indicated, the IT administrators cannot figure out what really happened in half of the insider incident cases. Proving who did what is another difficult issue for the respondents. Before discovering all the facts behind an insider incident, starting the termination process would increase the risk of expensive litigation. Therefore, it is often better to remediate than to make a quick termination.

The starting point for remediation should be to ensure all insiders, including employees, customers, and other business partners, understand organizational policies regarding use of the system. When a new user account is created for an employee or a business partner, there should be security training. The current employees and business partners should be subject to similar training at certain intervals. Employees should be trained to detect or notice suspicious activities. The consequences of policy violations should be clearly stated, and a signed document should be collected from each participant of the annual training sessions.

An anonymous tip line may encourage employees to report suspicious activities of colleagues when they are not sure. We should remember that most major security violations usually start with small, innocent-looking "accidental" violations. If there is no immediate response from the security management, the violations may get more serious. Any delay in responding will tempt the user to experiment further to test the grounds for bigger violations. To stop

TABLE 3. Most Adverse Consequences of InsiderIncidents Reported by the Respondent

Loss of confidential/proprietary data	11%
Reputational harm	11%
Critical system disruption	8%
Loss of current or future revenue	7%
Loss of customers	6%

Source: SEI. 2014. U.S. State of Cybercrime Survey. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

the growth of the violation into a bigger violation, any rule violation should be responded to quickly.

To eliminate the chances for accidental disclosures of sensitive material, and to improve information sharing, some organizations employ a color-coded mechanism called *Traffic Light Protocol (TLP)*. TLP is a simple, intuitive schema for indicating when and how sensitive information can be shared. For instance, a red symbol indicates that the recipients of this information may not share this information with any parties outside the specific meeting or conversation in which it was originally disclosed. Similarly, an amber symbol indicates that the recipient of this information can share it with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm (Schneier, 2005).

According to the U.S. Computer Emergency Readiness Team, TLP definitions are:

TLP:RED	Not for disclosure, restricted to participants only
TLP:AMBER	Limited disclosure, restricted to participants' organizations
TLP:GREEN	Limited disclosure, restricted to the community
TLP:WHITE	Disclosure is not limited

The following is an additional list of best practices to deter the insider threat and limit the potential damage (Cappelli, 2012):

- Identify high value and sensitive data and processes. Restrict access to sensitive, high-value data.
- Develop and implement insider threat policies and procedures with the help of human resources, legal counsel, security, and internal audit departments. Establish an insider threat group to maintain a readiness state.
- There must be an enterprise-wide policy for new accounts and strong passwords. Multi-factor authentication should be implemented and password files should be encrypted. Password sharing must be prohibited.
- New employee, contractor, and partners should be trained regularly in security awareness. There must be periodic changes in passwords.
- After a background check, all new employees, contractors, and business partners should be required to sign a nondisclosure agreement before they start working for the enterprise. In case of mergers and acquisitions, similar steps should be taken for the newly joined employees, contractors, and business partners.
- When an employee resigns or retires, an exit interview must be conducted. When a privileged user, such as system administrator or DBA, is terminated, he or she should be escorted out of the building immediately and all accounts associated with that user, especially the remote access accounts (including the cloud services), should be frozen immediately.
- All recent outgoing emails, attachments, print jobs, and downloads of the terminated employee should be reviewed carefully.

- The distribution of the company-owned equipment to various users should be documented, and when the employment is terminated, they should be returned.
- The help desk should not create new accounts.
- There must be a record keeping for the accounts reset, and these records should be reviewed.
- There must be restrictions to access the system in terms of time and location. Time and location of each access, and the process employed for each person (e.g., printing), should be logged.
- Backup tapes and backup processes should be limited to certain IT personnel. After encrypting, the backup media must be stored off-site. The encryption keys should be maintained in a secure location. The transportation of backup data and restoring from the backups should not be handled by the same persons. The effectiveness of the backup and restore functions should be tested regularly.
- Remote access and use of personally owned devices should be prohibited. Use of devices with cameras should be forbidden in sensitive areas.
- When there is a change in job definition or role, the access privileges should be re-evaluated to prevent privilege creep. Privileges should be determined on the need-to-know basis for each job and role.
- The privileged users, such as system administrators, should use different accounts when they perform non-privileged work. Activities of privileged workers should be monitored carefully. Use audit logs to detect the activities of employees outside their normal scope of work.
- An easy-to-use, anonymous reporting system for suspicious activities should be established.
- Annual refresher training on system security and insider threat should be provided for employees, especially senior management, contractors, and partners. The consequences of policy violations should be stated clearly.
- The enterprise-owned physical assets, and their ownership, should be maintained. The type of data or processes that can be employed on those devices should be specified.
- The data on all company-owned mobile devices should be encrypted.
- The rule for data and process ownership should be determined at the departmental level. Access rights to the data and processes should be determined by the data owner, not by IT.
- The required segregation of duties should be determined by the data owner.
- Periodic credit checks of employees should be used to identify the changes in the financial situation of employees. Within the boundaries of privacy laws, the human resources department should notify related managers when an employee's life situation (such as drug addiction or bankruptcy, etc.) deteriorates.

- Management should avoid favoritism, discrimination, and injustice in promotions and opportunities for growth.
- If a service provider is used, the service provider's security practices should exceed or improve the organization's own security practices. In simple terms, the use of a service provider, including the cloud service provider, should not add an additional risk to the organization.
- Any changes in the information system, e.g., network and hardware configurations, updates to operating system and applications, should be reviewed by system administrators, data owners, and users before they are implemented.
- The computer network must be monitored to establish what is normal behavior for an intrusion-detection system (IDS).
- Determine the ports and protocols needed and used regularly. Routers, modems, and firewalls must be configured to meet these demands.
- The virtual private network (VPN) access should be granted for certain hours and certain applications. The VPN access to foreign countries should not be given if there is no legitimate business need.
- The use of social media must be regulated within the scope of the existing legal system. A training program for security procedures, including teaching the risks associated with the improper use of the social media, must be provided to all users. An easy-to-use mechanism to report suspicious activities on social media must be established.
- The use of printers, scanners, fax machines, and copiers should be monitored.
- The use of certain data transfer mechanisms, such as FTP, should be restricted and anomalies should be reviewed.
- If there is no need for the transfer of data to other systems, the removable media should be eliminated. Printing or downloading sensitive documents should be restricted and monitored.
- Highly sensitive information should only be available at certain locations. Outside pre-specified locations, the encryption key should not be functional.
- There must be an enterprise-wide risk assessment of all systems, data, and processes, including the service providers.

CONCLUSION

Except in rare instances, the typical insider threat is a result of sophisticated technical hacker tools. Whether intentional or not, most insider incidences are either misused or abused privileges by a human being. Therefore, a human behavioral detection methodology is needed to understand the logic of the insider. In this aspect, collaborating with the HR department can provide the information needed by IT managers. With training provided by HR, IT managers can learn to notice how psychosocial factors—like a stressful divorce, difficulty working with others, or retaliatory behavior—may affect the insider threat.

References

BBC News. 2017, May 16. Chelsea Manning: Wikileaks Source and Her Turbulent Life. http://www.bbc.com/news/world-us-canada-11874276

Cappelli, D. M. 2012. The CERT Top 10 List for Winning the Battle Against Insider Threats. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=52423 Cisco. 2018. Cisco IOS NetFlow. https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html

CERT. 2014. 2014 State of Cybercrime Survey Presentation. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=298318Collins, M. L., Theis, M. C., Trzeciak, R. F., Strozer, J. R., Clark, J. W., Costa, D. L., Casidy, T., Albrethsen, M. J., and Moore, A. P. 2016. *Common Sense Guide to Mitigating Insider Threats,* 5th ed. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=484738

Costa, D. 2017. CERT Definition of 'Insider Threat'—Updated. https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html

Cushing, T. 2017, May 23. FBI Insider Threat Program Documents Show How Little It Takes to Be Branded a Threat to the Agency. Tech Dirt. https://www.techdirt.com/articles/20170517/12422437396/fbi-insider-threat-program-documents-show-how-little-it-takes-to-be-branded-threat-to-agency.shtml

Dark Reading. 2013, March 1. 5 Lessons from the FBI Insider Threat Program. Dark Reading. http://www.darkreading.com/vulnerabilities---threats/5-lessons-from-the-fbi-insider-threat-program/d/d-id/1139281?

FBI. n.d. Publications: Publications and Documents Relating to Counterintelligence. https://www.fbi.gov/investigate/counterintelligence/publications

FBI. n.d. Recent Insider Theft Cases [brochure]. https://www.fbi.gov/file-repository/insider_threat_brochure.pdf

FBI. 2011, February 11. Chinese National Sentenced for Stealing Ford Trade Secrets. https://archives.fbi.gov/archives/detroit/press-releases/2011/de041211.htmIBM. 2016, July 27.

IBM Security Tackles Insider Threats with User Behavior Analytics [press release]. https://www-03.ibm.com/press/us/en/pressrelease/50241.wss

Imperva. 2018. Privileged User Monitoring. https://www.imperva.com/Resources/PrivilegedUserMonitoring

Lawler, R. 2017, June 7. Judge Denies Uber's Request for Stay in Waymo Suit. Tech Crunch. https://techcrunch.com/2017/06/07/uber-waymo-lawsuit-stay-denied

Lovejoy, K. G. 2006, April 12. The Enemy Inside. CSO. https://www.csoonline.com/article/2120631/access-control/the-enemy-inside.html

Magklaras, G. B., Furnell, S. M., and Brooke, P. J. 2006,Towards an Insider Threat Prediction Specification Language. *Information Management & Computer Security, 14*(4) 361–381.

Moscaritolo, A. 2009, January 29. Disgruntled Fannie Mae Insider Indicted for Cyber Intrusion. SC Media. https://www.semagazine.com/disgruntled-fannie-mae-insider-indicted-for-cyber-intrusion/article/555400/

Office of the Director of National Intelligence. n.d. Insider Threat. https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-insider-threat

Richards, K. 2013, March 5. RSA 2013: FBI Offers Lessons Learned on Insider Threat Detection. https://searchsecurity.techtarget.com/news/2240179082/RSA-2013-FBI-offers-lessons-learned-on-insider-threat-detection

Schneier, B. 2005, December 19. Insider Threat Statistics. Schneier on Security. https://www.schneier.com/blog/archives/2005/12/insider_threat.html

SEI. n.d. Cybercrime Survey Collection. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. http://www.cert.org/insider-threat/research/cybersecurity-watch-survey.cfm?

SEI. n.d. Insider Threat. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. www.cert.org/insider-threat/

Shackleford, D. 2010. Keys to the Kingdom: Monitoring Privileged User Actions for Security and Compliance. https://www.sans.org/reading-room/whitepapers/analyst/keys-kingdom-monitoring-privileged-user-actions-security-compliance-34890

Special Issue on Insider Threat Modeling and Simulation. 2016, April. *Computational and Mathematical Organization Theory.* http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=455170

Tutorialspoint. 2018. Unix/Linux—File Permission/Access Modes. https://www.tutorialspoint.com/unix/unix-file-permission.htm

US-CERT. n.d. Traffic Light Protocol (TLP) Definitions and Usage. https://www.us-cert.gov/tlp

Wikipedia. n.d. Edward Snowden. https://en.wikipedia.org/wiki/Edward_Snowden

Wilber, D. Q. 2016, February 4. Stealing White: How a Corporate Spy Swiped Plans for DuPont's Billion-Dollar Color Formula. https://www.bloomberg.com/features/2016-stealing-dupont-white

Wilber, D. Q. 2016, February 8. So Began a 20-Year Course of Conduct of Lying, Cheating, and Stealing. *Bloomberg Businessweek (North America)*. http://www.pressreader.com/Canada/bloomberg-businessweek-north-america/20160208/282286729303079/