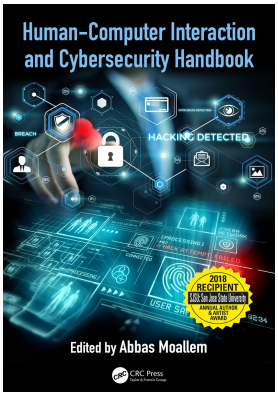

Human-Computer Interaction and Cybersecurity Handbook

Abbas Moallem

Insider threat

Publication details
https://test.routledgehandbooks.com/doi/10.1201/b22142-6
Maria Papadaki, Stavros Shiaeles
Published online on: 24 Oct 2018

chapter six

Insider threat

The forgotten, yet formidable foe

Maria Papadaki and Stavros Shiaeles

Contents

6.1 Nature of the insider threat

As a way of introduction, it would be useful to consider what the security community considers the insider threat to be and how it manifests itself. Mukherjee et al. (1994) define the *insider threat* as that who has legitimate access to the system but is abusing their privileges. Schultz (2002) subsequently considers insider attacks as deliberate misuse by those who are authorized to use computers and networks and identifies insiders as employees, contractors, consultants, temporary helpers, or personnel from third-party business partners. He pointed out how little was understood on insider threats at the time and discussed the many misconceptions that surrounded the issue. Bishop and Gates (2008) go a step further by considering insider threats in the context of trust and security policies, where levels of trust are expressed in a set of access control rules, which are in turn represented in a security policy. Specifically, they provide the following definition for an *insider*:

> A trusted entity that is given the power to violate one or more rules in a given security policy ... the insider threat occurs when a trusted entity abuses that power.... An insider can thus be defined with regard to two primitive actions:
> 1. violation of a security policy using legitimate access, and;
> 2. violation of an access control policy by obtaining unauthorized access.

Recognizing the lack of understanding in the area and the need for further research, Carnegie Mellon Computer Emergency Response Team's (CERT) research program began in 2000 with a US Department of Defense sponsorship on insider threats in military

services and defense agencies. Since then, their research has expanded to documenting more than 1000 insider threat case files, constituting the CERT Insider Threat Database, which provide technical, behavioral, and organizational details of each crime (Cappelli et al. 2012; Collins et al. 2016). Based on this knowledge, CERT's definition of a malicious insider is as follows (Silowash et al. 2012):

> A malicious *insider is* defined as a current or former employee, contractor, or business partner who meets the following criteria: i) has or had authorized access to an organization's network, system, or data; ii) have intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

Apart from malicious deliberate insiders, Hunker and Probst (2011) also recognize the significance of accidental threats and define an *insider* as an entity of trust who misuses their privileges, deliberately or accidentally, in a way that constitutes a threat. The CERT Insider Threat Center also recognizes unintentional insider threats and further elaborates by providing the following definition (Collins et al. 2016; Federal Infrastructure Protection Bureau 2013):

> An unintentional insider threat is defined as a current or former employee, contractor, or business partner who meets the following criteria:
>
> who has or had authorized access to an organization's network, system, or data and who, through their action/inaction without malicious intent cause harm or substantially increase the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.

In considering these definitions, it is relevant to note the various aspects that they encompass, legitimate access that is misused, the level of trust that leads to a security policy violation, the roles within an organization where this level of trust could be abused, the actions and intentions that could constitute a threat, and the potential impact to an organization's security. One could argue that all are correct, but each reflects a different dimension. They could even indicate how our understanding of the problem has evolved over time.

How about the range of threats that insiders could pose? Of the 1000 insider threat cases in the CERT Insider Threat Database, 734 involved malicious insider attacks (these cases did not include espionage or unintentional damage) (Collins et al. 2016). According to the same source, malicious insider attacks can be categorized into the following four classes:

- *Information technology (IT) sabotage*: an insider's use of IT to direct specific harm at an organization or an individual
- *Theft of intellectual property (IP)*: an insider's use of IT to steal IP from the organization; this category includes industrial espionage involving outsiders

- *Fraud*: an insider's use of IT for the unauthorized modification, addition, or deletion of data (not programs or systems) of an organization for personal gain or theft of information that leads to an identity crime (e.g., identity theft or credit card fraud)
- *Miscellaneous*: cases in which the insider's activity was not for IP theft, fraud, or IT sabotage

6.2 Significance of the problem

Having defined insider threats, it is important to understand how significant they are and why we need to care. Let us initially look at the number and frequency of insider attacks. Intel Security (2015) revealed that insiders were responsible for 43% of data loss incidents, half of which were malicious, and half, accidental. Ponemon Institute's 2014 survey reported that 88% of respondents believed the risks from privileged user abuse would increase within the subsequent 12–18 months. This was confirmed at Ponemon Institute's (2015) more recent study on the cost of cybercrime, which showed a 6% increase in frequency for malicious insider threat. Specifically, 41% of companies experienced malicious insiders, up from 35% the year before. Nonetheless, malicious insiders were, in fact, the least frequent attack type. In contrast, malware infections were at the top of the list and had affected 98% of respondents.

However, this does not necessarily mean they can be easily ignored. When it came to reviewing the cost of attacks in relation to their frequency, the order was almost reversed. Malicious insiders proved to be the costliest with an average annual cost of $167,890, whereas malware was featured at the penultimate position with the cost of $5,110. As the longer it takes to resolve an attack, the costlier it becomes, perhaps it is not surprising that the estimated average time to resolve different attack types also featured malicious insiders at the top with an average of 51.5 days, as opposed to 5.6 days needed for malware infections (Ponemon Institute 2016).

Looking at how each class might have affected different industry sectors, it is worth looking at Figure 6.1, which shows the three main insider threat classes, namely, IT sabotage, fraud, and IP theft, against the top six infrastructure sectors, as reported by CERT (Collins et al. 2016). We can see that financial motivation has been more prolific, mainly affecting the banking, finance, and local government sectors. Fraud has consistently featured as the top motivation even in previous editions of the study (Silowash et al. 2012). According to the 2016 Global Fraud Survey by the Association of Certified Fraud Examiners, which covers more than 114 countries globally, it is estimated that typical organizations lose 5% of their revenue to fraud each year. One fifth of the reported cases caused losses of at least $1 million. Interestingly, it is also reported that most of the fraudsters are first time offenders with clean employment histories (ACFE 2016).

Apart from fraud, IP theft and sabotage seem to feature at equal weights (Collins et al. 2016). IP theft has affected IT and healthcare sectors to a larger degree than others. Additionally, sabotage has been more prominent in the IT sector. Lastly, the banking and finance industry seems to have had the largest share of reported malicious insider cases, standing with twice as many incidents as the second sector, IT. Does this mean that the banking and finance industry is a prime target? Before rushing to such conclusion, it is worth considering the different legislative requirements on mandatory reporting across industries. Perhaps we are more aware of insider incidents in some industries, rather than others, due to such different notification requirements. In the absence of mandatory reporting in some sectors, it would be fair to suspect that the number of reported incidents only reflects the tip of the iceberg.

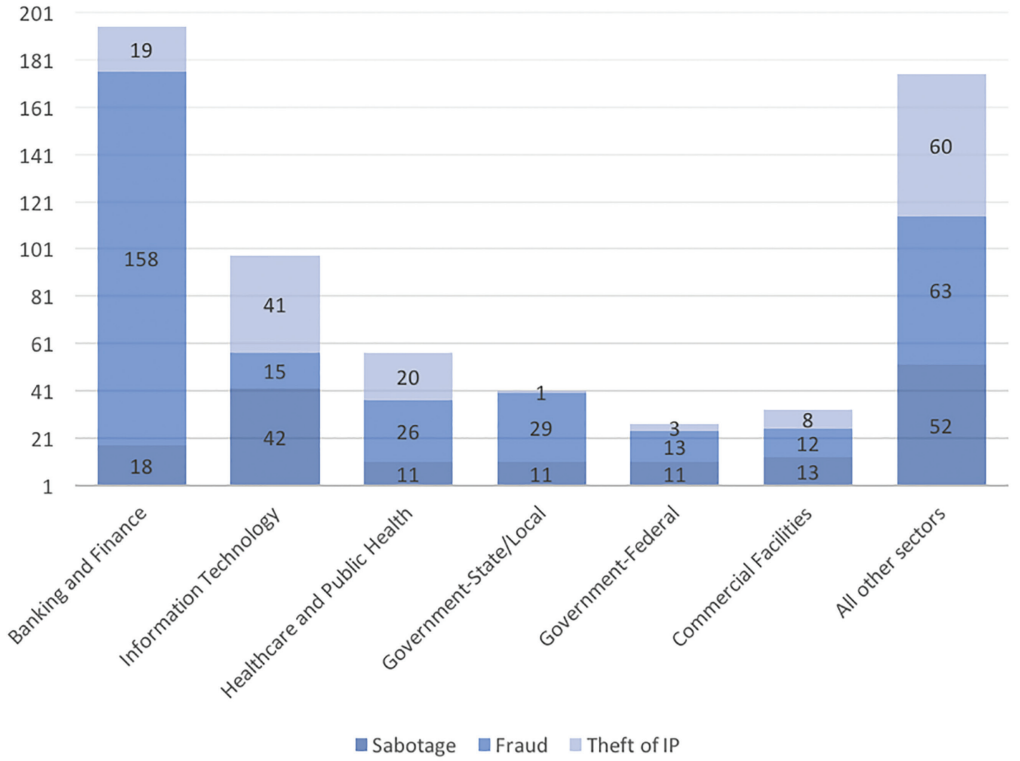

Figure 6.1 Top six infrastructure sectors for sabotage, fraud, and IP theft. (Data from Collins, M. et al., *Common Sense Guide to Mitigating Insider Threats*, Technical Report CMU/SEI-2016-TR-015, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2016.)

Further supporting this view, evidence from the 2014 US State of Cybercrime Survey reveals that 75% of respondents handled insider incidents internally, without involving legal action or law enforcement (PWC 2014). When asked about the reasons for not reporting, the answers raised concerns about their readiness to do so, as the lack of evidence and inability to identify the individual(s) responsible featured in the top two answers.

As such, if three out of four incidents are handled internally, without involving legal action or law enforcement, then perhaps it is worth reviewing the Verizon Data Breach Investigations Report, which is based on validated real data, reported and unreported, from 65 contributing organizations across the globe, including the CERT Insider Threat Center. Other participating organizations are Akamai, Checkpoint, Cisco, Dell, Kaspersky Lab, Mcafee, Qualys, etc. Their dataset provides approximate 95% confidence level for each statement (Verizon 2017). The 2016 Verizon report is based on more than 10,000 insider incidents and gives insight into the motivation behind insider threats. Although financial motives remain prominent with 34%, the gradual rise of espionage over time suggests that the threat landscape is changing (Verizon 2016).

Interestingly, when looking at organizations' discovery timeline for insider and privilege misuse, this is more likely to take months and years, rather than weeks or days (Verizon 2017). A highly reported insider case falls right into this category. It involved a decade of economic espionage within Canadian telecommunications company Nortel by Chinese hackers, leading to Nortel's ultimate collapse in 2009. It demonstrates the

impact of insider threats and showcases the difficulties in detecting and responding to them. According to Brian Shields, Nortel's former senior systems security advisor, hackers stole at least seven passwords from top executives and subsequently downloaded sensitive information, including business plans, research and development reports, as well as employee e-mails. Suspicious activity was discovered in 2004, when a personal computer (PC) was found to be regularly sending sensitive data to Shanghai. Further investigation found evidence of insider attacks dating as far back as 2000. However, Nortel seized the internal investigation 6 months later, due to lack of progress and resorted to simply changing affected user passwords. Mike Zafirovski, Nortel's chief executive at the time, played down the importance of the breach, allowing it to carry on for years. Shields was certain that the extensive espionage attacks contributed to Nortel's downfall, and he is not alone in this view (CBC News 2012; Leyden 2012). Why did it take Nortel 4 years to detect that something was wrong? Is insider threat detection a technically difficult task or was Nortel lacking an appropriate insider threat program? Perhaps both are true. Ultimately, Nortel's consistent reluctance to acknowledge and address the significance of the problem led to their eventual demise and paved the path for the global dominance of Chinese telecoms competitors.

One could argue that high-profile cases, such as Nortel's attacks, have helped raise the profile of insider threats and have helped us understand their significance. More high-profile cases will be reviewed in Section 6.3. Perhaps, it is worth reviewing how organizations perceive the significance of the insider threat. The levels of concern among organizations seem to be rising, which might suggest that attitudes and priorities toward insider threats could soon be changing. Indeed, 89% of respondents in the 2015 Vormetric Insider Threat Report believed they were at risk, and one out of three felt very or extremely vulnerable. Reassuringly, 92% of respondents are planning to increase or maintain existing spending on IT security, whereas only 11% feel that their organization is safe (Vormetric 2015). The 2016 Insider Threat Spotlight report reveals similar findings (Schulze 2016). Specifically, three out of four organizations felt vulnerable to insider threats, and one in three felt very or extremely vulnerable.

6.3 *Insider threats in practice*

Having reviewed the significance of the insider threat and how it affects organizations, we also discussed the decade-long espionage attacks against Nortel. It is worth reviewing the literature for other high-profile cases, which attracted the media's attention and brought insider threats to the spotlight. It seems that IP theft cases are the most widely reported stories. The most notable example is that of Edward Snowden, a former US National Security Agency (NSA) contractor, who revealed the extent of the Internet and phone surveillance by US intelligence (BBC 2013). Snowden, a computer wizard without formal education, initially joined the US Central Intelligence Agency (CIA), working on IT security. He quickly rose through intelligence ranks, taking up a diplomatic post in Geneva in 2007. After leaving CIA in 2009, he subsequently worked as a US NSA contractor, through outside contractor consultancy, Booz Allen. As part of his role, he had access to sensitive information, which he downloaded and eventually handed to journalists. According to Szoldra (2016), he downloaded 1.5 million sensitive files from the NSA before fleeing the country, handing the documents to journalists in Hong Kong and eventually obtaining asylum in Russia. Since then, journalists have released 7000 of these documents, which represent only a small subset of the original set. Unsurprisingly, Snowden was fired from Booz Allen in June 2013 and has been charged by the US government and NSA for the

unauthorized communication of national defense information and willful communication of classified communications intelligence. Snowden admitted in an interview that he only took the job at Booz Allen to obtain access to classified information and obtain evidence (BBC 2013). Nonetheless, looking beyond the exposed secrets, the organizations and individuals involved, which have certainly raised eyebrows and have attracted intense media attention, there are questions to be had on the insider threat. For example, how sensitive information was handled, how trust was managed with third-party contractors, and ultimately what detection and prevention mechanisms were put in place to mitigate information leakage. Wikileaks informant Manning (BBC 2017), as well as the leak of customer information at the Target incident, also received significant media attention and helped raise the profile of insider threats (Upton and Creese 2014).

Other cases motivated by IP theft involve Mike Yu (Reuters 2011a) and Kexue Huang (Reuters 2011b). Yu, a product engineer at Ford Motor Company during 1997–2007, was arrested in October 2009—and sentenced to 70 months in prison—on the basis of stealing a large number of secret documents from the company. According to the US Attorney's office, Yu accepted a job at the China branch of a US company in December 2006. However, before he notified Ford about his new job, Yu copied approximately 4000 sensitive documents onto an external hard drive, including sensitive design documents about engine transmission and electric power supply systems. Yu gave his termination notice to Ford via an e-mail from China and eventually worked for a Chinese automaker (Reuters 2011a). In a similar fashion, Kexue Huang led a scientific team developing organic insecticides at Dow Chemical Company subsidiary and subsequently for another multinational company, Cargill Inc. Huang was charged for stealing trade secret from Dow and Cargill, which he then transferred to China and Germany, giving them competitive advantage by saving them millions of dollars and years in research and development. The estimated losses from Huang's case ranged from $7 to $20 million (Reuters 2011b).

Sergey Aleynikov (WSJ 2015), a former Goldman Sachs programmer, stole the company's secret source code of high-frequency trading platform and was sentenced to 8 years in prison. During his last few days at the company, he transferred 32 MB of proprietary computer code, which could have cost his employer millions of dollars. Although he attempted to hide his activity, the company detected it through anomalies in its network monitoring system. In the last example of IP theft, Michael Mitchell (Steinmeyer 2010), a former engineer and salesman of DuPont, is a typical example of a disgruntled insider. After being terminated because of poor performance, Mitchell kept the numerous numbers of DuPont computer files and proprietary information, which he eventually used when he accepted a consultancy position at DuPont's Korean competitor. The case was discovered only when he attempted to contact current and retired DuPont employees to gather even more secrets, but ended up being reported by some employees instead. This example shows how insider cases could take a long time to be discovered by investigators.

One case of IT sabotage, as reported by CERT Insider Threat Center, involved a computer support technician, who had administrator-level password-controlled access to the organization's network. Three months after leaving the company, they logged in late at night using the administrator account to remotely access the organization's network. They changed the passwords of all other IT system administrators and shut down nearly all the organization's servers. They also deleted backup files, which could have enabled the organization to recover more smoothly. As a result, the organization and its customers were unable to access its services and data for days. As a result, the insider was arrested and convicted to a $30,000 penalty, almost 2 years in prison, and community service (Collins et al. 2016).

This case highlights the need for robust employee termination procedure, which could have removed or locked the employee's credentials.

Lastly, an example of preventable fraud case is provided by Collins et al. (2016). An employee embezzled $200,000 from their organization, a bookkeeper business, by writing checks from the organizational account to pay for personal expenses. They also modified the organizational records to hide their tracks and show different payees. The incident took place over 2 years and was only discovered through irregularities in the electronic check ledger. The insider was convicted for this crime, but the funds were never recovered. As it transpired, the same person had been convicted for similar fraud in the past, so background checks before hiring could have prevented this attack (Collins et al. 2016).

6.4 Detecting insider threats

Despite the fact that intrusion detection systems were initially conceived with the aim of detecting both internal and external attacks, the reality of detecting insider threats has proven to be more challenging. According to Schulze (2016), when asked about the difficulty of detecting and preventing insider attacks as opposed to external attacks, 66% of respondents found them to be more difficult, and only 7% thought they were easier. Specifically, respondents attributed the main challenges in effectively detecting and responding to the following parameters:

- Insiders already have credentialed access to the network and services (67%).
- There is increased use of applications with potential to leak data (i.e., web, e-mail, cloud data stores, and social media) (53%).
- Increased amount of data that leaves protected boundary/perimeter (46%).
- More end user devices capable of theft (33%).

This section will review the main approaches of detecting insider threats, drawing on their advantages and limitations.

6.4.1 Log and system analysis approaches

Magklaras and Furnell (2001) suggest a structured approach at predicting insider misuse by considering the insider's sophistication level, historical behavior, and their motivation. Its foundation is the insider threat prediction model (ITPM), which initially estimates the potential impact of the incident, as well as the suspected insider's role, the hardware and software tools they are capable of using, their historical behavior, etc. The resulting outcome will help predict the threat level from intentional and accidental insider incidents. Although largely theoretical, and not fully implementable at the time, ITPM presents interesting concepts and links the threat level (and hence possible outcome) to the attacker's level of sophistication.

In a similar fashion, Maybury et al. (2005) concentrate on highly sophisticated malicious insiders and propose an insider threat detection model, which distinguishes motives, actions, and associated observables. Observables for cyberactions include network, system, information reconnaissance, access to assets (e.g., media, hosts, and accounts), entrenchment (e.g., installing sensors or unauthorized software), exploitation (e.g., commanding and controlling entrenched assets such as software bots or zombie machines), extraction and exfiltration (e.g., of hardcopy, media, and information), communication (e.g., encrypted messaging, encoded messages, and covert channels), manipulation of cyberassets

(e.g., changing file permissions and suppressing or altering information content), counterintelligence (e.g., wiping disks), and other cyberactivities associated with unethical or addictive behavior (e.g., online gambling). They test their approach against three types of malicious insiders, namely, an analyst, application administrator, and system administrator, involving a wide range of motives (e.g., financial, thrill, or ideological). The behavior of these three insiders is simulated and captured on MITRE's demilitarized zone network, which already has 75 online active users during the 3-month evaluation period. A heterogeneous and multilevel data collection approach is adopted, incorporating physical (e.g., card access records), network (e.g., Snort IDS, Stealthwatch, honeynet, and e-mail sensors), host (e.g., logins and password updates), and application [e.g., e-mail, secure shell (SSH), and web server logs] level data. The Common Data Repository (CDR) is the result of this evaluation, containing more than 11 million anonymized records. The proposed system is tested against the CDR and evaluated based on its accuracy and timeliness. The accuracy is determined in relation to false positives and false negatives, whereas timeliness is considered as the difference between the time malicious activity begins, the time it is put on a watch list, and the time an insider threat alarm is triggered. Stealthwatch alerts included an element of human analysis, whereas all other methods were autonomous. The goal of the proposed system is to reduce the time between defection to discovery from years and months to weeks and days. Their results are encouraging, as two insiders were detected within 1 week, and the third was detected within 2 weeks. Also, the heterogeneous, multilevel data collection and fusion approach is interesting. However, it is difficult to draw generic conclusions, based on three simulated case studies.

Agrafiotis et al. (2014) have focused on characterizing employee behavior based on their role within the organization. They use activity trees and sequentially based analysis for users in similar roles, where activity trees include the range of activities that an employee (potential insider) may conduct as part of their expected daily workload. A similarity measure indicates how branches compare to others, and detection is based on identifying unusual new activity branches with similarity between them and existing branches below a certain threshold. It is based on sequential tree-based profiling, through a proof-of-concept software tool that builds the tree profile, measuring the similarity of newly observed branches and seeing results. This concept is an extension to the general idea of attacking trees, which incorporates the sequence of events that will result in attack. Attack trees are the first tier of a tree system, which can provide insight into the objectives of internal attacks, receiving information about the attackers, and formulate a hypothesis about the occurrence of an attack. Behavior trees can reflect dynamic behaviors including patterns of conducts. The system is written in Python programming, which facilitates entering new set of data and achieving a dynamic approach.

The corporate insider threat detection (CITD) system is designed for large-scale data repositories and activity logs and incorporates user- and role-based profilings. It combines technical activities and behavioral actions to assess the threat posed by individuals (Legg et al. 2015). It is an anomaly-based detection system, which compares a user's observed behavior against their user and role profiles, flagging significant deviations. User and role profilings feature selection concentrates on unusual device, activity, and attribute access. For example, one observation could be that an e-mail was sent (activity) to john .davis@mycompany.com (attribute) from PC-012 (device). The CITD is designed to operate in supervised and unsupervised modes, where the feedback from a human analyst can significantly help reduce false alarms. The experimental results using various synthetic datasets in unsupervised mode have been highly encouraging, and its deployment and evaluation on a large multinational corporation is expected in the future.

Liu et al. (2005) also proposed an anomaly detection system for insider threats. It aims to apply anomaly detection methodologies, widely used for external threats, to the domain of insider threat detection. The proposed methodology consists of three steps: data collection, feature extraction, and internal threat detection using the *k*-nearest neighbor algorithm. Three types of feature collection are used to evaluate the performance of the proposed methodology: *n*-grams of the programs used, the frequency with which the programs are executed, and the parameters given in the executable programs. The *k*-nearest neighbor algorithm belongs to the supervised learning class. Supervised learning algorithms assume that it is possible to collect training data that is totally free from malicious actions or real data containing the label of normal or malicious energy. Such a case in the case of detecting internal threats can be fatal. Liu et al.'s (2005) paper outlines the insider threat detection method, which tracks system calls at the operative level to monitor inside level to monitor activity. The system calls have a higher degree of information reliability due to the capacity of monitoring *all* system activity, and the monitoring becomes more closely attached into the operating system, becoming more demanding in the user permissions to access, use, or delete monitoring information without traces of tampering.

A comparison between non-upervised and supervised learning techniques for detecting masquerading attacks is investigated by Wolff (2010). Two nonsupervised techniques were used, specifically the minimum distance technique and the compact cluster technique. A synthetic dataset of 15,000 system calls per user over a 6-month period, including synthesized masquerade data, was used for the comparison (Schonlau et al. 2001). The focus is on two classes of insiders, specifically masqueraders and traitors. The training dataset contains the first 5,000 calls for each user, whereas the remaining 10,000 calls were split into blocks of 100 commands each to create 100 blocks for each user. Initially, the unsupervised algorithms were compared. The unsupervised algorithms are used to take into consideration all the users' history when generating a user profile, while the supervised algorithm considers only a preestablished set of data. The basis for the nonsupervised learning techniques of the author is the minimum distance, which is a technique proposed for the creation of a user profile, based on the premise of the minimum distance algorithm aiming to find the block of data closer to other blocks of individual's user dataset. To attain it under a nonsupervised algorithm, the author makes adjustments to the uniqueness algorithm, removing the update technique because the user profiling algorithm is already controlled by all data when creating a profile, eliminating the need for dynamic updating of the profile while classifying the data. The results were promising for unsupervised approaches. For small to medium classification thresholds, supervised algorithms outperformed the others, but for the larger thresholds of 400 anomalous blocks, unsupervised methods matched those of supervised ones.

Salem et al. (2008) also conducted a comparison of different machine-learning techniques, for insider threat, using the same Schonlau dataset (2001). Specifically, they tested against the following algorithms: uniqueness of commands; Bayes one-step Markov approach based on one-step transitions from one command to the next; a hybrid multistep Markov method; compression method based on differences in compressing test data from the same user rather than a masquerader; a similarity measure for each sequence command; incremental probabilistic action modeling (IPAM); naive Bayes classifier; semiglobal alignment; Eigen cooccurrence matrix (ECM); and self-consistent naive Bayes classifier, which combines naive Bayes and the EM algorithm. Their experimental results are shown in Table 6.1. It is fair to say that no algorithm clearly outperforms all the others, whereas using a combination of approaches seems to yield marginally better results. The Schonlau dataset has limited scope and is therefore insufficient to reflect true insider

Table 6.1 Accuracy of machine-learning techniques in insider threat detection

Method	False alarms (%)	Missing alarms (%)
Uniqueness	1.4	60.6
Bayes one-step Markov	6.7	30.7
Hybrid multistep Markov	3.2	50.7
Compression	5.0	65.8
Sequence match	3.7	63.2
IPAM	2.7	58.9
Naive Bayes (updating)	1.3	38.5
Naive Bayes (no updating)	4.6	33.8
Semiglobal alignment	7.7	24.2
ECM	2.5	28.0
Naive Bayes + EM	1.3	25.0

Source: Salem, M.B. et al., A survey of insider attack detection research, In Stolfo, S.B. et al. (Eds), *Insider Attack and Cyber Security*, Springer, Boston, MA, 2008, pp. 69–90.

threat detection rates. However, it is still useful in comparing different machine-learning techniques.

As seen earlier, applying machine-learning techniques for insider threat detection can have various degrees of success. As insider threat behavior can vary widely, it is difficult to characterize it without considering the human factor. It is often approached as a generic anomaly detection task, where a combination of multiple techniques is likely to yield slightly better results. Chandola et al. (2012) provide a comprehensive review of various anomaly-detection approaches in generic intrusion-detection scenarios and note that most techniques deal with univariate discrete sequences. To understand online and multivariate sequences, more needs to be done. It would be interesting to investigate the applicability of deep learning approaches and whether they could produce better results. One such approach is that of Tuor et al. (2017), who use deep belief networks against the CERT Insider Threat Dataset v6.2 (Glasser and Lindauer 2013). Their approach considers normal behavior for a user, a role, or a project team and inspects the stream of system logs to infer user metadata and network activity. Their research is still in the early stages, but it does highlight the potential for further research in the area.

6.4.2 *Psychological and technical approaches*

Looking into the human factor, the opportunity in psychological models is a widely used feature for detecting insider threats (Gheyas and Abdallah 2016). In order to determine the level of this opportunity and identify or mitigate the attack, most studies focus on two broad categories of features: the role of the internal threat in the system and activity-based characteristics. A significant part of this research is conducted around the psychological profiling of company employees. The outline of the psychological profile enables the user's history to be recorded as well as the psychological status at specific times.

Under the psychological approach, the theoretical work of Kandias et al. (2010) states that an attack is highly dependent on three main factors: motivation, ability, and opportunity. The authors study the psychosocial perspective and the implications of the prediction of the insider threat through the use of social media, under open-source intelligence, and the content generated by the user, through an inductive methodology. The model is based on the assumption that psychological traits, such as negative beliefs toward authority,

can be monitored through the use of social media tools, and those who hold such beliefs are more prone to be insider intruders given the opportunity. As such, it focuses on detecting users with a negative attitude toward authorities by profiling social media channel YouTube. They used a free flat representation data technique to target the user's attitude and improve the scalability of their method. Their research showed a correlation between psychological traits and malevolent insiders. The advantage of such model lies in the ease of gathering data, which are mostly public, and the fact that YouTube is a space where users tend to show their opinions. Apart from the privacy concerns of monitoring employees' social media data, another weakness resides on the fact that it cannot demonstrate with clarity the escalation of behavior, from malevolent attitude toward authority to the actions that cause an internal threat.

The work of Greitzer et al. (2010) combines traditional cybersecurity audit data and psychosocial indicators that can be used to predict internal threats. They also consider legal and ethical issues in the type of activity that one could collect in an organizational context. Traditional cybersecurity audit data, which consist of events that are normally used to determine policy violations or outlier behavior, are incorporated with demographic/organizational data about the employee. Information sources that informed various psychosocial factors included staff performance evaluations, competency tracking, disciplinary tracking, timecard records, proximity card records, and preemployment background checks. The proposed approach still raises privacy issues on employee monitoring, which could lead to more disgruntlement toward the organization and eventually more severe malicious insider events. On the other hand, it is possible for an organization to fall into the "trust trap," where the longer employees stay in an organization, the safer the organization feels about them, giving them a false sense of security.

Brdiczka et al. (2012) also use a combination of psychological profiles (PPs) with structural anomaly (SA) detection from social and information networks. SA uses graph analysis, dynamic tracking, and machine learning to detect anomalies, whereas PPs are dynamically constructed from behavioral patterns. Outcomes from both SA and PP are fused and ranked to detect insider threats, targeting the reduction of false positives and false negatives at the same time. The creation of dynamic psychological profiles uses observable indicators to reflect the emotional state and personality of a perpetrator. As such, they are based on psychometric assessments (e.g., extraversion) and temporal work patterns. The analysis includes online and PC usage behaviors, sentiment analysis of a user's communications, and social network features and analysis. The authors argue that creating a psychological profile has the effect of shrinking the volume of data as well as reducing false alarms. Quite interestingly, the proposed approach was tested on a real dataset retrieved from a multiplayer online game, World of Warcraft (WoW), and consisted of behavior traces of over 350,000 game characters over a 6-month period. Although the data are not derived from an organizational context, the authors claimed that their approach showed promising results and could be used to predict when characters would quit their guild (a form of gaming club) and cause possible damage to their group. One could argue that there are similarities between insiders in an organization and WoW players. Still, the proposed method has not been tested against organizational real data yet, and hence, it is difficult to evaluate its applicability in corporate scenarios.

Legg et al. (2013) also attempted to achieve the detection of internal threats through surveillance techniques and psychological tests, developing a conceptual model that incorporates an all-encompassing organizational view of the problem. The novelty is the priority rankings, known as lanes. There are four *lanes*, namely, enterprise, people, technology and information, and physical. Initially, users are ranked based on the level of access they

hold, as well as using psychological tests. Psychological tests try to detect the user's level of knowledge, whether they have a predisposition for illegal energy and whether the user has high levels of stress. This is combined with real-time collected data, which feed into the decision-making system to extract the level of risk for each user. According to the authors, the algorithm that should be used in the decision-making system is different for each organization, depending on the data that each organization decide to use. The conceptual model is three dimensional and incorporates in descending order the following tiers: hypothesis, measurement, and real world. The analyst in charge of detecting potential insider threats is put above the hypothesis tier, capable of supervising all the tiers below it. The real-world tier contains sets of elements, such as activity logs, building access logs, and psychological mind-set among others. The measurement tier records measures of real-world elements, whereas the hypothesis tier relies on these measurements to test different hypotheses. The model considers high levels of confidence for directly observable elements, such as system access logs for the measurement of whether an insider could have downloaded sensitive IP. Psychological elements, such as the stress level of an employee, are only observable by an indirect mode based on a small set of indicators, therefore providing lower confidence level. The output of the model is the probability of the hypothesis being true. This reasoning-based model is important, as it allows the analyst to explore and test different hypotheses based on suspicions for specific employees, while it allows the hypotheses to be formed by the underlying reasoning component from the real-world tier.

While previous approaches have associated personality traits with social media behavior, Alahmadi et al. (2015) concentrated on web-browsing behavior. Their hypothesis is that the detection of insider threats could be based on the linguistic features of the websites users regularly visit. As such, they suggest that the detection of insider threats could concentrate on the user's Internet browsing behavior and the associated personality traits used for the detection of insider attacks. The associated personality traits include the OCEAN (openness, conscientiousness, extraversion, agreeableness, and neuroticism) and the dark triad (Machiavellianism, narcissism, and psychopathy) characteristics. The foundation of the proposed research is to consider how browsing behavior relates to personality traits and how browsing behavior deviates over time to proactively identify potential insider threats, before significant damage is caused. To this end, the proposed system collects the content of each website. Irrelevant content from the retrieved hypertext markup language (HTML) source code is initially removed (e.g., HTML and JavaScript tags), and then relevant keyword features are extracted, such as money, loan, debt, hire, tax, and love. The resulting dataset is passed through an algorithm calculating its dimensions and is then fitted to a *k*-means algorithm that tries to extract the personality traits of the user. The combination of user personality traits can indicate if a user is likely to be an insider threat, whereas the deviation of such behavior can signal an internal threat. The benefit of such model is the possibility of calculating the probability of deviant behavior based on widely available information.

Apart from psychological profiling, and the technical or behavioral indicators of potential attacks, Nurse et al. (2014) also consider the wider context of an attack and specifically the motivations of malicious attackers as well as human factors affecting unintentional incidents. They propose a framework for conceptualizing and characterizing insider attacks, based on four areas, namely, *catalyst*, *actor characteristics*, *attack characteristics*, and *organization characteristics*. The proposed framework identifies a catalyst as a key event, which could tip the insider over the edge into committing the offense. Catalyst events include, among others, the following: demotion, dismissal, dispute with employees, family

problems, blackmail, a new job offer, or even the lack of training in unintentional attacks. Actor characteristics encompass the following: psychological state, personality traits, attitude toward work, motivation to attack, skill set, opportunity to attack, as well as previous history of rule violations. Dark triad traits Machiavellianism, excitement seeking, and narcissism were more closely related to malicious actors, whereas OCEAN traits (especially agreeableness and openness) can indicate susceptibility to scams. Overall, significant attention is given toward understanding the propensity to attack and how it could be influenced by different elements. The proposed framework recognizes that none of these elements in isolation is sufficient to detect insider attacks. However, in combination, they could provide invaluable insight into characterizing and understanding insider threats.

To understand the attack itself, one could consider elements, such as the overall objective, as well as the specific steps and goals needed to achieve the attack. For example, an attack that plants a logic bomb could be driven by revenge and have the objective to sabotage a company's mission-critical function. In the case of unintentional threats, the business task, which was the reason for the activity, could be considered the attack objective. For example, a time-critical task, which has to be completed within strict time constraints, could lead an employee to copy sensitive data on a universal serial bus (USB) key and subsequently lose them in public transport. As for attack steps and goals, in a similar fashion to attack trees, they represent the individual steps that are needed to achieve the attack. For example, in order to steal sensitive IP, an insider might follow several stages: initially gather intelligence on who has access credentials; figure out a way of extracting them through blackmail, charm, financial means, etc.; extract credentials to access sensitive information; and finally cover their tracks. The last area within the framework includes organization characteristics, such as assets under attack and their vulnerabilities. Several known scenarios from the CERT Insider Threat Dataset and the United Kingdom's Centre for the Protection of National Infrastructure were successfully characterized. The authors also used an additional set of cases within their broader research, as directly collected by Whitty and Wright (2013). Overall, although not a detection system in itself, the proposed framework is very useful in understanding different elements and contextual factors influencing insider attacks.

The potential of informing insider threat detection with psychological and psychosocial factors can be beneficial and a significant body of research has informed insider threat detection with personal characteristics of potential insiders. It is particularly useful as it has the potential to proactively identify potential insiders and escalate monitoring and response before any significant damage is caused. Psychological and psychosocial characteristics alone are not enough to identify insider attacks, but if combined with suspicious behavior, opportunities, and catalysts, they could play an important role in insider threat detection. However, a significant challenge of these approaches is that their accuracy is heavily influenced by the availability of such data. Quite often, psychological profiles might not be readily available within organizations or even shared across different departments. Although personality traits and psychological features can be dynamically inferred from online user behavior, there are still privacy issues with such approaches at various degrees (Greitzer et al. 2010). Although one could argue, for example, that monitoring online browsing data would pose fewer privacy concerns than social media activity, the potential for employees' privacy to be invaded cannot be ignored. As such, organizations and solutions would need to consider the ethical and legal issues surrounding the issue. Although far-fetched, another consideration is how malicious insiders, who are aware of the importance of psychological profiling in insider threat detection within an organization, could potentially modify their online behavior accordingly to evade monitoring

controls. Despite these concerns, it is important to recognize that insider threat detection can be greatly enhanced by considering the human factor and its strong relationship with the propensity to attack.

6.5 Best practices for insider threat mitigation

Preventing and detecting insider threats is a complex issue, especially as malicious insider online activity is often similar to what insiders do as part of their normal role. Hence, it is important to recognize that the mitigation of insider threats cannot involve technical controls alone and cannot be the sole responsibility of the IT and security personnel (Cappelli et al. 2012). Instead, best practice guidelines require the cooperation of management, human resources, legal, physical security, data owners, information technology, and software engineering (Collins et al. 2016). Organizations are advised to adopt the following 20 best practice guidelines, which will enable them to prevent, detect, and respond to such threats effectively, incurring as little costs and disruption as possible. Specifically, these guidelines and practices are summarized in the following (Collins et al. 2016):

1. *Know and protect your critical assets*: This includes identifying and protecting all assets that provide the organization with a competitive advantage. As a quick win solution, organizations are advised to conduct physical assets inventory, understand what data the organization process, identify the software configurations of all assets, and prioritize assets and data to identify high-value targets.
2. *Develop a formalized insider threat program*: A formalized insider threat program provides designated resources to deal with the problem and allows the effective prevention, detection, and response to insider incidents. An insider threat program needs to consider issues, such as whom to involve, who has authority, whom to coordinate with, whom to report to, what actions to take, and what improvements to make.
3. *Clearly document and consistently enforce policies and controls*: All organizational policies should include a clear and consistent message that aims to reduce the chance of employees damaging or lashing out at the organization for a perceived injustice. Policies and punishments ought to be fair and consistent and not disproportional to the violation that occurred. Quick win solutions for enforcing and advocating this clear message include the following: adoption of policies and practices by everyone, including senior management; regular briefing of all employees on policies and procedures, accompanied by signing of acceptable use and/or nondisclosure agreements; making policies and procedures easily accessible to all employees; making annual refresher training mandatory for all employees; and facilitation of clear and concise enforcement of policies, free from favoritism and injustice.
4. *Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior*: Organizations should proactively deal with suspicious or disruptive employees, as this could reduce the risk of insider threats. This could include a thorough background investigation on criminal or credit records, encouragement of employees to report suspicious behavior, and investigation and documentation of incidents involving suspicious or disruptive behavior.
5. *Anticipate and manage negative issues in the work environment*: Additional monitoring of employees with an impending or ongoing personnel issue, based on consistent organizational policies and procedures, will allow easier detection and response to a potential insider incident. User privacy would need to be considered, and access to such logs would need to be on a need-to-know basis. Additionally, organizational

changes would need to be communicated clearly and transparently to allow them to better plan for their future.

6. *Consider threats from insiders and business partners in enterprise-wide risk assessments*: This practice includes a comprehensive risk-based security strategy for the protection of critical assets against internal and external threats, including trusted business partners. High-impact solutions would include nondisclosure agreements upon hiring and termination of employment or contracts, enforcing background investigation of business partner employees, performing background checking against all employees to be acquired during company merging or acquisitions, preventing unnecessary printing of sensitive documents, avoiding direct connections of business partners to information systems, and restricting access to backup systems only to relevant employees.
7. *Be especially vigilant regarding social media*: Policies, training, and procedures ought to define how employees, contractors, and business partners should use social media to avoid intentionally or unintentionally threatening critical assets. Apart from providing social media policy and training program, users can be encouraged to report suspicious e-mails or phone calls to the information security team.
8. *Structure management and tasks to minimize insider stress and mistakes*: An organization is encouraged to provide an environment conducive to positive behavior, by understanding the psychology of employees and the demands placed upon them. For example, establish success metrics that are relevant and appropriate to the work environment; encourage focusing on one thing at a time rather than multitasking; offer opportunities for employees to destress; routinely monitor employee workloads to ensure that they are appropriate; and encourage employees to think through projects, actions, and statements before committing to them.
9. *Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees*: Periodic security training for employees and contractors will support a successful security culture within the organization. An anonymous or confidential reporting mechanism of security incidents will also help toward this goal.
10. *Implement strict password and account management policies and practices*: This aims to prevent malicious insiders from circumventing manual and automated control mechanisms by compromising user accounts. Account management policies, strong password selection requirements, training on secure password practices, access to shared accounts on a need-to-know basis, and regular auditing of account creation and password changes would help toward this practice.
11. *Institute stringent access controls and monitoring policies on privileged users*: Privileged users have the technical ability to commit and conceal malicious activity, so organizations should conduct periodic reviews to avoid privilege creep and ensure that they follow the principle of least privilege as employees change roles.
12. *Deploy solutions for monitoring employee actions and correlating information from multiple data sources*: Relying on network activity alone is not enough, as the number of data sources could significantly enhance insider threat analysis and response. Relevant technical and nontechnical data sources could include among others authentication logs, firewall logs, telephone records, file access logs, physical access records, performance evaluations, physical violation records, or travel reporting.
13. *Monitor and control remote access from end points, including mobile devices*: Remote access is often perceived by insiders as a less risky option. Also, mobile workforce and employees' own devices often connect via the same route. Monitoring remote access, disabling it once an employee or contractor leaves the organization, considering the

use of personal devices in the risk planning, and limiting the use of cameras in sensitive areas are relevant good practices.

14. *Establish a baseline of normal behavior for both networks and employees*: Building on from practice 12, it is good practice to analyze the collected data to establish normal behavior per role and deviations from these profiles. Network behavior could include bandwidth utilization, usage patterns, and protocols, whereas employee behavior could encompass typical working hours, resource usage patterns, and resource access patterns.
15. *Enforce the separation of duties and least privilege*: In a similar fashion to privileged users, account management ought to consider the separation of duties and follow the principle of least privilege, especially as they change roles.
16. *Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities*: Data access control and monitoring ought to be included in any agreement with cloud service providers. In addition, good practices include risk assessment for any data or services that are subject to cloud outsourcing, verification of the cloud service provider's hiring process, and remote access restrictions to hosts providing cloud services.
17. *Institutionalize system change controls*: Change management controls across systems and applications could help prevent the introduction of backdoors, keystroke loggers, or logic bombs. In addition, the periodic review of configuration baselines could help discover any undocumented discrepancies.
18. *Implement secure backup and recovery processes*: Regular backup processes will enhance the ability of an organization to recover from incidents and enhance its resilience. Maintaining off-site backups and including network infrastructure devices in the backup and recovery plans are both good practices.
19. *Close the doors to unauthorized data exfiltration*: Understanding data exfiltration vulnerabilities is important to establish relevant mitigation strategies. USB flash drives, printers, cloud, and e-mail are relevant vectors, each with its unique challenges. Relevant practices include establishment cloud computing policy; monitoring of printer, fax, copier, scanner usage; defining of data transfer policy; defining of and enforce removable media policy; and restricting of data transfer protocols, such as file transfer protocol and SSH file transfer protocol.
20. *Develop a comprehensive employee termination procedure*: Termination procedures should ensure that all accounts are closed, access tokens and equipment are collected, remaining personnel are notified, and nondisclosure agreements are reaffirmed.

6.6 Conclusions

The problem of insider attacks cannot be ignored, as the Nortel case highlights. The insider threat might not be as frequent as malicious software, but its impact can be costly. Our understanding of the insider threat problem, the relevant indicators, and how various factors can influence one another are increasing. Still, the detection of insider threats is more likely to take months and years, rather than hours and days. Although attitudes are starting to change, and organizations have started to recognize the significance of the issue, they are still a long way from adopting successful insider threat programs. In terms of detection, the research community has concentrated on both technical and hybrid solutions. Detecting insider threats is not a purely technical solution, and the human factor can play an important role. Recent research has recognized its importance and has incorporated personality traits, psychological and psychosocial data, as well as motivations and

possible catalysts of insider events. Beyond prevention and detection, though, best practices and guidelines recognize that insider threat is a multifaceted problem, and the success of insider threat mitigation strategies depends on the cooperation of various groups within an organization. Specifically, specific emphasis is given on management, human resources, legal, physical security, data owners, IT, and software engineering.

References

ACFE (Association of Certified Fraud Examiners). *Global Fraud Study: Report to the Nations on Occupational Fraud and Abuse*. ACFE, Austin, TX (2016). Available at: https://s3-us-west-2.amazonaws.com/acfepublic/2016-report-to-the-nations.pdf.

Agrafiotis, Ioannis, Philip Legg, Michael Goldsmith, and Sadie Creese. Towards a user and role-based sequential behavioural analysis tool for insider threat detection. *Journal of Internet Services and Information Security* 4, no. 4 (2014): 127–137.

Alahmadi, Bushra A., Philip A. Legg, and Jason R. C. Nurse. Using Internet activity profiling for insider-threat detection. In *International Conference on Enterprise Information Systems* (2), (2015), pp. 709–720.

BBC. Profile: Edward Snowden. (2013). Available at: http://www.bbc.co.uk/news/world-us-canada-22837100.

BBC. Chelsea Manning: Wikileaks source and her turbulent life. (2017). Available at: http://www.bbc.co.uk/news/world-us-canada-11874276.

Bishop, Matt, and Carrie Gates. Defining the insider threat. In *Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead*. Association for Computing Machinery, New York (2008), p. 15. Available at: http://nob.cs.ucdavis.edu/bishop/papers/2008-csiiw/definsider.pdf.

Brdiczka, Oliver, Juan Liu, Bob Price, Jianqiang Shen, Akshay Patil, Richard Chow, Eugene Bart, and Nicolas Ducheneaut. Proactive insider threat detection through graph learning and psychological context. In *2012 IEEE Symposium on Security and Privacy Workshops (SPW)*. Institute of Electrical and Electronics Engineers, Piscataway, NJ (2012), pp. 142–149.

Cappelli, Dawn M., Andrew P. Moore, and Randall F. Trzeciak. *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. Addison-Wesley, Boston, MA (2012).

CBC News. Nortel collapse linked to Chinese hackers. (2012). Available at: http://www.cbc.ca/news/business/nortel-collapse-linked-to-chinese-hackers-1.1260591.

Chandola, Varun, Arindam Banerjee, and Vipin Kumar. Anomaly detection for discrete sequences: A survey. *IEEE Transactions on Knowledge and Data Engineering* 24, no. 5 (2012): 823–839.

Collins, Matt., Michael Theis, Randall Trzeciak, Jeremy Strozer, Jeremy Clark, Daniel Costa, Tracey Cassidy, Michael Albrethsen, and Andrew Moore. *Common Sense Guide to Mitigating Insider Threats*, 5th Edition (Technical Report CMU/SEI-2016-TR-015). Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA (2016). Available at: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=484738.

Federal Infrastructure Protection Bureau. *Unintentional Insider Threats: A Foundational Study*. (Technical Report CMU/SEI-2013-TN-022). Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA (2013). Available at: http://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf.

Gheyas, Iffat A., and Ali E. Abdallah. Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis. *Big Data Analytics* 1, no. 1 (2016): 6.

Glasser, Joshua, and Brian Lindauer. Bridging the gap: A pragmatic approach to generating insider threat data. In *Security and Privacy Workshops (SPW) 2013*. Institute of Electrical and Electronics Engineers, Piscataway, NJ (2013), pp. 98–104.

Greitzer, Frank L., and Deborah A. Frincke. Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. In Probst, Christian W., Jeffrey Hunker, Dieter Gollmann, and Matt Bishop (Eds), *Insider Threats in Cyber Security*. Springer, New York (2010), pp. 85–113.

Hunker, Jeffrey, and Christian W. Probst. Insiders and insider threats—An overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 2, no. 1 (2011): 4–27. Available at: http://isyou.info/jowua/papers/jowua-v2n1-1.pdf.

Intel Security. *Grand Theft Data: Data Exfiltration Study*. McAfee, Santa Clara, CA (2015). Available at: https://www.mcafee.com/us/resources/reports/rp-data-exfiltration.pdf.

Kandias, Miltiadis, Alexios Mylonas, Nikos Virvilis, Marianthi Theoharidou, and Dimitris Gritzalis. An insider threat prediction model. In *International Conference on Trust, Privacy and Security in Digital Business*. Springer, Berlin (2010), pp. 26–37.

Legg, Philip A., Nick Moffat, Jason R. C. Nurse, Jassim Happa, Ioannis Agrafiotis, Michael Goldsmith, and Sadie Creese. Towards a conceptual model and reasoning structure for insider threat detection. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 4, no. 4 (2013): 20–37.

Legg, Philip A., Oliver Buckley, Michael Goldsmith, and Sadie Creese. Caught in the act of an insider attack: Detection and assessment of insider threat. In *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*. Institute of Electrical and Electronics Engineers, Piscataway, NJ (2015), pp. 1–6.

Leyden, J. Whistleblower: Decade-long Nortel hack "traced to China." *The Register*. (2012). Available at: https://www.theregister.co.uk/2012/02/15/nortel_breach/.

Liu, Alexander, Cheryl Martin, Tom Hetherington, and Sara Matzner. A comparison of system call feature representations for insider threat detection. In *IAW'05. Proceedings from the Sixth Annual IEEE SMC: Information Assurance Workshop*. Institute of Electrical and Electronics Engineers, Piscataway, NJ (2005), pp. 340–347.

Magklaras, George B., and Steven Furnell. Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers & Security* 21, no. 1 (2001): 62–73.

Maybury, Mark, Penny Chase, Brant Cheikes, Dick Brackney, Sara Matzner, Tom Hetherington, Brad Wood, Conner Sibley, Jack Marin, and Tom Longstaff. *Analysis and Detection of Malicious Insiders*. Mitre Corporation, Bedford, MA (2005).

Mukherjee, Biswanath, L. Todd Heberlein, and Karl N. Levitt. Network intrusion detection. *IEEE Network* 8, no. 3 (1994): 26–41.

Nurse, Jason R. C., Oliver Buckley, Philip A. Legg, Michael Goldsmith, Sadie Creese, Gordon RT Wright, and Monica Whitty. Understanding insider threat: A framework for characterising attacks. In *2014 IEEE Security and Privacy Workshops (SPW)*. Institute of Electrical and Electronics Engineers, Piscataway, NJ (2014), pp. 214–228.

Ponemon Institute. *Privileged User Abuse and the Insider Threat*. Commissioned by Raytheon Company, Independently conducted by Ponemon Institute LLC. Ponemon Institute, Traverse City, MI (2014).

Ponemon Institute. *2016 Cost of Cyber Crime Study and the Risk of Business Innovation*. Sponsored by Hewlett Packard Enterprise. Ponemon Institute, Traverse City, MI (2016). Available at: http://www.ponemon.org/local/upload/file/2016 HPE CCC GLOBAL REPORT FINAL 3.pdf.

PWC (PricewaterhouseCoopers). *US Cybercrime: Rising Risks, Reduced Readiness*. PWC, London (2014).

Reuters. Ex-Ford engineer sentenced for trade secrets theft. (2011a). Available at: http://www.reuters.com/article/us-djc-ford-tradesecrets-idUSTRE73C3FG20110413.

Reuters. Chinese man pleads guilty for US trade secret theft. (2011b). Available at: http://www.reuters.com/article/us-crime-china-theft-idUSTRE79H78R20111018.

Salem, Malek Ben, Shlomo Hershkop, and Salvatore J. Stolfo. A survey of insider attack detection research. In Stolfo, Salvatore J., Steven M. Bellovin, Angelos D. Keromytis, Shlomo Hershkop, Sean W. Smith, and Sara Sinclair (Eds), *Insider Attack and Cyber Security*. Springer, Boston, MA (2008), pp. 69–90.

Schonlau, Matthias, William DuMouchel, Wen-Hua Ju, Alan F. Karr, Martin Theus, and Yehuda Vardi. Computer intrusion: Detecting masquerades. *Statistical Science* 16, no. 1 (2001): 58–74.

Schultz, Eugene E. A framework for understanding and predicting insider attacks. *Computers & Security* 21, no. 6 (2002): 526–531.

Schulze, H. *Insider Threat: Spotlight Report, Crowd Research Partners Report*. (2016). Crowd Research Partners. Available at: http://crowdresearchpartners.com/wp-content/uploads/2016/09/Insider-Threat-Report-2016.pdf.

Silowash, George, Dawn Cappelli, Andrew Moore, Randall Trzeciak, Timothy J. Shimeall, and Lori Flynn. *Common Sense Guide to Mitigating Insider Threats*, 4th Edition (No. CMU/SEI-2012-TR-012). Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA (2012). Available at: http://resources.sei.cmu.edu/asset_files/technicalreport/2012_005_001_34033.pdf.

Steinmeyer, Peter A. *Former DuPont Employee Sentenced to 18 Months For Trade Secret Misappropriation*. (2010). Epstein Becker & Green, P.C. Available at: http://www.tradesecretsnoncompetelaw.com/2010/03/articles/trade-secrets-and-confidential-information/former-dupont-employee-sentenced-to-18-months-for-trade-secret-misappropriation/.

Szoldra, Paul. This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks. *Business Insider UK* (2016). Available at: http://uk.businessinsider.com/snowden-leaks-timeline-2016-9.

Tuor, Aaron, Samuel Kaplan, Brian Hutchinson, Nicole Nichols, and Sean Robinson. *Deep Learning for Unsupervised Insider Threat Detection in Structured Cybersecurity Data Streams*. Artificial Intelligence for Cybersecurity Workshop at AAAI, North America (2017). Available at: https://aaai.org/ocs/index.php/WS/AAAIW17/paper/view/15126.

Upton, David M., and Sadie Creese. The danger from within. *Harvard Business Review*, September 2014 issue. (2014) Available at: https://hbr.org/2014/09/the-danger-from-within.

Verizon. *2016 Data Breach Investigations Report*, 9th Edition. Verizon, Basking Ridge, NJ (2016). Available at: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.

Verizon. *2017 Data Breach Investigations Report*, 10th Edition. Verizon, Basking Ridge, NJ (2017). Available at: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf.

Vormetric. *2015 Vormetric Insider Threat Report: Trends and Future Directions in Cyber Security*. Vormetric, San Jose, CA (2015). Available at: https://www.vormetric.com/campaigns/insiderthreat/2015/pdf/2015-vormetric-insider-threat-press-deck-v3.pdf.

Wall Street Journal. Ex-Goldman programmer guilty of stealing code. (2015). Available at: http://www.wsj.com/articles/jury-gives-split-verdict-in-trial-of-former-goldman-programmer-sergey-aleynikov-1430496291.

Whitty, Monica, and Gordon R. Wright. *Corporate Insider Threat Detection Internal Deliverable 3.1: Report of Findings from Case Studies*. University of Oxford, UK (2013).

Wolff, Matt. Unsupervised methods for detecting a malicious insider. *Proceedings of the 7th International ISCRAM Conference–Seattle* 2 (2010).