Insider Threat in Banking Systems

Chapter · September 2016

DOI: 10.4018/978-1-5225-0864-9.ch013

Qussai Yaseen
Ajman University

Online Banking Security Measures and Data Protection

Shadi A. Aljawarneh
Jordan University of Science and Technology, Jordan

A volume in the Advances in
Information Security, Privacy,
and Ethics (AISPE) Book Series

IGI GLOBAL
DISSEMINATOR OF KNOWLEDGE
www.igi-global.com

Published in the United States of America by
IGI Global
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Aljawarneh, Shadi, editor.
Title: Online banking security measures and data protection / Shadi A. Aljawarneh, editor.
Description: Hershey, PA : Information Science Reference, 2017. | Includes bibliographical references and index.
Identifiers: LCCN 2016028381| ISBN 9781522508649 (hardcover) | ISBN 9781522508656 (ebook)
Subjects: LCSH: Internet banking--Security measures. | Electronic funds transfers--Security measures. | Data protection. | Computer networks--Security measures. | Computer security.
Classification: LCC HG1708.7 .O55 2017 | DDC 332.1/7028558--dc23 LC record available at https://lccn.loc.gov/2016028381

This book is published in the IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) (ISSN: 1948-9730; eISSN: 1948-9749)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

Chapter 13
Insider Threat in Banking Systems

Qussai Yaseen
Jordan University of Science and Technology, Jordan

ABSTRACT

Insider threat poses huge loss to organizations since malicious insiders have enough knowledge to attack high sensitive information. Moreover, preventing and detecting insider attacks is a hard job because malicious insiders follow legal paths to launch attacks. This threat leads all kinds of attacks in banking systems in the amount of loss it causes. Insider threat in banking systems poses huge harm to banks due to the importance and attractiveness of assets that banks have. This chapter discusses insider threat problem in banking sector, and introduces important surveys and case studies that show the severeness of this threat in this sector. Moreover, the chapter demonstrates some policies, technologies and tools that may prevent and detect insider threat in banking systems.

DOI: 10.4018/978-1-5225-0864-9.ch013

INTRODUCTION

Insider threat is one of the riskiest threats that worry individuals and organizations. A malicious insider is a trusted insider who misuses his/her privileges in a system to hinder the system's operations, damage data, or disclose sensitive information which causes damage to the system. According to different surveys, such as the CSI survey (Richardson, 2010), Forrester Research (Forrester Research, 2010) and the ISBS survey (InfoSecurity Europe, 2010), insider threat causes huge harm to individuals and organizations. The CSI survey (Richardson, 2010) stated that the cost of data records lost to insider attacks is greater than the cost of those lost to outsiders. This is because insiders are familiar with the system, and attack the valuable records, while outsiders steal what they can access.

Financial institutions are especially subject to insider threats due to the highly sensitive stored information and their highly dependence on information technologies. According to CERT (Cappelli, Moore & Trzeciak, 2012), the financial sector suffers from the most cases of fraud, and the second most in IT sabotage and theft of intellectual property carried out by malicious insiders. Furthermore, there are non-malicious insiders who may pose risks unintentionally, through mistakes or bad behaviors that may be exploited by external parties. Non-malicious insiders may be fooled by some attackers to click on URL that contains malware, or may mistakenly send corporate materials to unauthorized recipients.

This chapter discusses the problem of insider threat in banking systems. It introduces the problem of insider threat in information systems and its growing threat. Furthermore, the chapter presents some survey results that show how risky is the insider threat. Next, the problem of insider threat in banking systems is introduced. Basically, the chapter discusses the special sensitivity of this problem in banking systems, and how insider threat poses high risk in this sector. Surveys results and case studies that show the increasing risk and loss posed by insider threat and threaten this sector are introduced. In addition, the chapter discusses how recent exposure of technologies such as Cloud Computing increased the threat and maximized the vulnerabilities that may be used by insiders to harm banking systems. Next, the technologies and tools used to fight insider threat in banking systems are introduced.

INSIDER THREAT

Insider threat is a critical security problem. The threat of insiders can be posed unintentionally or intentionally by malicious insiders. Malicious insider threat is defined as the threat that is caused by a person who has authorized access privileges and knowledge of the computer systems of an organization, and is inspired to antagonistically influence the organization (Brackney & Anderson, 2004). Insiders could be employees, contractors, or business partners. They have the capabilities, which outsiders do not have, that enable them to launch complicated attacks.

According to different surveys (Gordon, Loeb, Lucyshyn & Richardson, 2005; CERT, 2011), insider threat is as risky as outsiders' threat (hackers) due to the extreme harm that it may pose. The FBI Computer Crime Survey (Gordon, Loeb, Lucyshyn & Richardson, 2005) reported that trusted insiders were responsible of about 33% of all security breaches in 2005. Similarly, the Cyber Security Watch Survey (CERT, 2011) showed that 58% of attacks are caused by outsiders, whereas 21% of attacks are caused by insiders. Moreover, the survey shows that insider threat is as costly as outsider threat. However, Forrester Research (Forrester Research, 2010) showed that insider threat is the costliest type of incident. In addition, after analyzing the security practices of more than 300 European, American, and Australian enterprises, Forrester estimated that insiders were responsible for 75% of data security incidents in those enterprises in 2010. Similarly, Verizon Business breach report (Cooper, 2008; Subashini & Kavitha, 2010) stated that outsiders exposed about 30,000 records, whereas insiders exposed about 375,000 records indicating that the cost of insider threat is greatly more than the cost of outsider threat.

Obviously, many surveys have shown that insider threat is an immense and urgent security problem. Yet, organizations are investing very little to defend their systems against insider threat. Most organizations' investments are focused on protecting their assets from outsiders' threat. Organizations rely on insiders' morals and ethics not to violate systems security. Nonetheless, surveys show that this assumption is incorrect. Mechanisms that have been proposed for protecting data from outside attacks are inappropriate to secure systems from authorized users who may misuse their privileges. Therefore, the development of mechanisms that protect sensitive data from insiders has become a key demand due to the amount of harm that can be caused by malicious insiders.

Researchers in insider threat mitigation proposed some techniques for fighting insider threat at system level or application level such as relational databases. Many approaches focused on visualizing the capabilities an insider has through using graph based models. The purpose of this representation is to discover how knowledgeable an insider is and what risk s/he poses through his knowledge. The knowledgebase of insider may have the values of data items s/he recently accessed and read, or the information s/he gets when s/he read an object. In addition, the knowledgebase may contain the access rights s/he has on data items and the type of accesses such as read, write, etc. Furthermore, the knowledgebase may contain the dependencies among objects or data items that the insider knows.

Insiders may attack systems directly using their access privileges to attack systems components. They may rely on some techniques to hide their footprints, which enable them to harm the systems with small probability of discovering their attacks. Moreover, insiders may discover some vulnerabilities in the organization laws or installed countermeasures. They may use these flaws with their knowledge about other systems components to attack the systems.

Serious attacks may be launched by insiders using dependencies among data items or objects. Therefore, determining dependencies among data items or objects is a major part in handling insider threat. A dependency between two data item, components or objects A and B is defined as the existence of a relationship between their values. That is, we say that B depends on A, denoted by A→B, when the value of B depends on the value of A, and any change in the value of A will result in the B's value (Yaseen & Panda, 2012, 2009). Dependencies could be direct, as in the later example, or transitive. A transitive dependency among the data items, components or objects A, B and C, denoted by A→B→C exist when a change in A's value will result in a change in B's value, and in turn, this will result in a change in C's value. In this example, we say that C depends transitively on A, or there is a transitive dependency between A and C (Yaseen & Panda, 2012; 2009). Insiders may use these dependencies to launch attacks. For example, suppose that an insider, say Alice, has a read access to a data item A, where A is regular information. In addition, that the underlying system has the dependency A→B, where B is sensitive information that Alice should not access. Alice can infer information about B using the dependency A→B and her authorized access to A.

Dependencies among data items or objects could be naïve or complex. Naïve dependencies are easily detectable by systems designers or security officers. Therefore, they can take those dependencies into account when distributing access privileges to prevent insiders' attacks. However, some dependencies are complex, especially transitive dependencies, and may be discovered and used by malicious insiders. Therefore, security officers should pay too much attention to dependencies and what information insiders can get using these dependencies (Yaseen & Panda, 2012, 2009).

Insiders get knowledge about dependencies during their work in organizations' systems. They can get a part of the knowledge through their activities and transactions in systems. This accumulated knowledge enables insiders to discover the strengths and weaknesses of the defense mechanisms and the systems' structure. Nonetheless, outsiders have little information (in comparison to insiders) about the structure of the systems they attack. Moreover, insiders use legal paths to breach the systems' security throughout legal access, whereas outsiders rely on violating systems security using different methods such as bogus URLs in phishing attacks, SQL injection, Man-in-the Middle attacks, etc.

Insiders may launch standalone or collaborative attacks. Standalone attacks mean that an insider launch attacks alone using his knowledge and access privileges only. Meanwhile, collaborative attacks are launched by two or more insiders. In this type of attacks, insiders share their knowledge about the victim system, including dependencies, and use their access privileges to harm the system. Collaborative attacks may greatly harm organizations more than standalone attacks since the capabilities of collaborative insiders together are much more than the capabilities of individual insiders. However, most discovered insider attacks were launched by individual insiders. Obviously, collaborative attacks are harder to form since insiders need to talk together and agree about the attack. This process includes some risk that some insiders may need not to take.

INSIDER THREAT IN BANKING SYSTEMS

The world of banking has been changed dramatically in the last few years. The immense growth of information technology tools forms a major cause of this continuous change. Smart credit cards, online services, the spread of E-commerce applications, the outsourcing of information and applications, the cloud computing and the rapid growth of the number of third parties are few examples of this change. The fast speed networks and internet have made many networked applications applicable, and increased the spread of such applications among clients. Banks are in a race to provide a friendly and easy access services to clients. They invest large amount of money in building a technological infrastructure to achieve their goals. One aspect of technological change in how organizations dealing with their information is the increasingly relying on third party systems for storing information and providing many of digital services. Many banks find themselves in need to adapt such cloud services because of cost reduction, scalability and resources availability in the huge infrastructures of cloud providers. However, the technological evolution has brought major security concerns, especially in banking systems due to the high sensitive information that is processed in such sector.

The type of information is a major factor of its attractiveness to attacks. Information in banks such as credit card numbers, account numbers and budgets are targets for different types of attacks due to its high sensitivity. Outside attacks form the larger percentage of attacks of information in banking systems. The evolution of internet and networking has led to an immense growth on the number of attackers who can attack information systems in banks. Hackers around the world costs banking sector huge amount of money yearly due to credit cards stealing, money movements and financial compensations for clients. Therefore, highly cost countermeasures should be purchased, installed and updated to prevent, detect and mitigate cyber security attacks. In banking systems, the tradeoff between the costs of defense mechanisms and information leakage always pushes towards buying expensive security tools to mitigate security attacks and prevent information leakage.

Banks have to adapt new security policies and countermeasures because of the continuous change in attack tactics followed by intruders. According to the report issued by the New York Department of Financial Services (Cuomo & Lawsky, 2014), the cyber-attacks against banks are becoming more complicated, wide spreading quickly and increasing immensely. The report demonstrated that banks face different types of intrusions. Account takeovers forms 46% of cyber intrusions. Identity theft intrusions formed about 18% of cyber intrusions in the surveyed institutions. Telecommunication network disruptions and data integrity breaches were reported by 15% and 9.3% respectively. Breaches caused by third-party partners formed about 18% and 15% of small and large institutions, respectively. ATM skimming/point-of-sale schemes were reported by 23%, mobile banking exploitation (in large institutions) formed 15%, and insider access breaches were reported by 8% of intrusion incidents.

The stream of attacks costs financial sector a huge loss. According to US Government Accountability Office (United States Government Accountability Office USGA, 2015), information about the losses by U.S. depository institutions because of cyber-attacks is limited. The report demonstrated that some sources estimate the losses for about $23 millions of dollars in 2013. Moreover, the report says that the loss is increasing dramatically. However, the report assures that the loss is much more than this number because many institutions do not report their actual loss. Outside attacks by hackers forms a huge loss to financial sector. However, insiders form more harm to banks and the loss an insider causes to banking sector is much greater than a harm caused by a hacker.

The Risk of Insider Threat in Banking Systems: Surveys and Case Studies

Hackers are not the only threat to information systems in banking sector. Insider threat poses much more harm than outsiders. Insiders attacking banking systems costs banks a huge loss since insiders usually attack highly valuable information, while outsiders steal what they can access. The reason behind this result is that insiders are familiar with the technological infrastructure of banks. Moreover, they usually know where the valuable information is stored and how they can access it. In addition, insiders follow legal paths that are hardly traceable or detectable. Meanwhile, outsiders follow random paths and scan many ports before they succeed in attacking systems. These attempts can be detectable before a breach happens, and in most cases, they are easily detectable because of the footprints left.

Banking and financial sector leads all other sectors in insider threat, and has the greatest loss because of this problem. Many surveys showed the risk of insider threat in banking systems. A study by Carnegie Mellon University (Cummings, Lewellen, McIntire et al., 2012) examined 23 incidents of insider activity in the banking and finance sector. The study found that 91 percent of victim organizations suffered financial loss ranges from hundreds of dollars to hundreds of millions of dollars. According to a recent RSA presentation (Richards, 2013), in 10 years, the average loss per industry is $15 million, and the average cost per incident is $412,000. Moreover, the damage in many instances was more than $1 billion. However, many insider threat cases showed that the loss caused by insiders is terrifying and it is much greater than what was found in those surveys as will be discussed shortly.

The history of banking system is full of insiders' cases that have caused too much damage to banks. For example, Kweku Adoboli caused $2.3 billion in losses for UBS, Switzerland's biggest and most error-prone bank (Walker, 2012). In 2011, Adoboli used his knowledge of the bank system and infrastructure to create fake trades to hide his track. He bet the bank's money on the future price of various stock indices. To hide his crime, he created offsetting fictitious transactions. His knowledge as an insider helped him in taking advantages of some vulnerabilities of the securities law, and in using them for exchange-traded funds (ETFs) to book these factious transactions. As an employee in the front disk, he knew that ETFs rules do not require brokers to produce the confirmation of trades immediately. This rich information gave him the advantage to attack the system. Obviously, outsiders may not have this kind of information to launch this type of attacks.

The case of trader Bruno Iksil is another example about how insiders in banking sector could cause catastrophic loss to banks. In May 2012, Jamie Dimon, the CEO of JP Morgan Chase & Co, announced that the bank lost about $2 billion because of bad trades in London. After this announcement, the bank lost about $14 billion of its share price. This catastrophic loss was caused by the trader Bruno lksil or "the London Whale" as he is nicknamed. The "London Whale" took bad bets on a credit derivatives index. Later, Dimon discovered that this process caused the bank a loss of about $6.2 billion, not $2 billion as estimated early (Childs, 2013).

The cases discussed in the previous paragraphs are few examples of the risk of insider threat. Obviously, one insider threat case may cause loss greater than the loss caused by too many outsiders' attacks. Definitely, insider threat may be intentional or unintentional. However, in both cases, the loss in banks because of this threat is catastrophic. Therefore, suitable mechanisms are needed to mitigate this threat. To design, install and update insider threat countermeasures, security officers in banking sector should have a detailed knowledge about the approaches that insiders follow to attack systems.

Approaches of Insider Attacks in Banking Systems

Insider attacks are becoming frequent, more sophisticated and more harmful. Continuously, insiders develop new types of attacks to bypass countermeasures. Moreover, some organizations do not invest enough money to defend their systems against insider threat. Most investments focused on protecting organizations systems against hackers. They usually rely on insiders' ethics and morals to not harm systems, which is a wrong assumption and proved by many surveys and insider attacks cases.

The method of attack may be determined by the type of target. Some attacks used insider privileges to get unauthorized benefit without harming clients' accounts. Other attacks target clients' accounts. The most prominent target in banking systems is the attacking of Personally Identifiable Information (PII) of clients (Cummings, Lewellen, McIntire et al., 2012), which is account number, credit or debit card number, in addition to any required security code, access code, or password. However, some attacks do not involve PII. This section discusses some approaches that were used by insiders to attack banking systems.

Attacking Banking Policies

The first type of attack discussed here does not target clients, and is performed by a high privileged insider. The insider in this type targets banks using the loans policy. In this attack, an insider, say Alice, has an access to loans database. She has the read and write privileges in this access. Alice applies for a loan in her bank, which approves her request according to the bank policy. Alice gets an amount of X money as a loan. Later, Alice uses her privileges several times to maliciously increase her personal loan amounts, and withdraws the resulting difference and removes essential loan documentation to hide the fraud.

An example of this attack is the case discussed in an interesting study conducted by CERT program in Carnegie Mellon University. In that case, an insider working at the loan department at a bank applied for two legitimate loans of $39000 in total. The bank approved her loans according to the bank policy. Later, she used her full privilege in reading and modifying loans to increase her loans amount several times and withdrew the difference. To hide her crime, she removed essential loans documentation. Totally, the insider stole $112,000 using this approach. Fortunately, her crime was discovered during a routine audit, which found missing loan documents from her account.

Attacking Personally Identifiable Information (PII)

The second type of attacks targets the Personally Identifiable Information (PII) as described previously. In this attack, the insider uses his/her privileges in viewing clients PII to copy and use it fraudulently. The insider can exploit his/her access to the PII of clients in various malicious ways. For example, s/he can use the information in purchasing items on internet, or s/he can change the address of a client and issue a new credit card and send it to the new address and use it later. Moreover, the insider can use an outsider and give him/her the PII of some client. Next, the outsider can make fake identification using the PII information and withdraws fund from the victim account. Real stories about this type of attack are provided next.

The first example took place in New York, where an insider in a bank printed the account information of several clients and gave it to her boyfriend. Using his friends, her boyfriend talked with a homeless man who agreed to enter some of the bank branches posing as legitimate account holders and withdraw fund from their accounts. The total losses because of this crime exceeded $235,000.

The second example is about criminals who were ordinary customer service employees at a bank call center. Surprisingly, the employees had access to customer information including PII. Using their legitimate access, they printed customer records and gave them to an outsider who used them to make purchases. In some cases, the insiders changed the address of some customers and issued credit cards which were sent to the new incorrect address. Later, they used the new credit cards to perform some purchases. The estimate loss that was caused by this fraud was about $2.2 million.

The last example about this type was conducted by a branch manager of a national bank. The father of the manager branch, which had a criminal history, persuaded his son to conduct identity theft scheme in collaboration with the father's friend (outsider). The outsider asked the manager to steal the account information of some customers using his privileges, and offered him $1,000 for each account information. Using a team of complicit cashiers, the outsider made fake identifications using the account information to fraudulently withdraw funds. The total losses because of this fraud in a period of three months were $228,000.

Non-Technical Attacks

Banks may suffer insider threat in non-technical cases. Although the focus of this chapter is on technical attacks, non-technical attacks are discussed briefly in this chapter. This type of attacks spans many attack areas such as stealing cash from drawers. A good example of this type is what demonstrated in CERT study about insider threat in financial sector. In this example, a temporary employee was responsible for placing large cash deposits in the vault in bank-issued deposit bags. The insider created fake bags using the bank system, and put them in place of legal deposit bags, and stole the money from the legal bags. During a period of three months, the insider succeeded to steal about $92,000 (Cummings, 2012).

Insider Threat Mitigation in Banking Systems

Defending banks information systems against insider threat require robust prevention, detection and recovery countermeasures. Preventive countermeasures should raise alerts and prevent insiders before committing a crime. Despite the fact that the concept of prevention is clear in information security, designing and applying these controls is not an easy job in insider threat mitigation. The majority of insiders are employees who perform normal daily tasks in the system. An insider threat prevention countermeasure should take into account the tradeoff between allowing insiders to perform their tasks and stopping insiders' tasks that are considered attacks to the underlying system.

Insider Threat Prevention

Adopting good access control models in banking systems is crucial to prevent insider threat. Insiders, despite the job level they have, should be allowed to access authorized information. Moreover, insiders should get access to the minimum number of data items needed to perform his/her task. The aforementioned principle is called the *Least Privilege*. Applying this rule limited or prevented the damage of insider threat cases in many financial organizations. Another important rule in insider threat prevention is called *Separation of Duties*. An insider who has too much access and privileges is a high risky insider. For example, consider an insider, say John, who has write access to loans and can modify the log file in a bank. John can fraudulently change the amount of loans and remove his record from the log file, or modify it to trap other insiders. The rule Separation of Duties is a very important rule, which reduce the probability of insider attacks by removing or mitigating the capability of one insider to harm the system. Moreover, restricting access to PII and applying good monitoring system on PII or other sensitive information increase the probability of preventing insider attacks or reduce the damage that may occur in systems because of attacking such valuable information. Furthermore, good sanction policies may reduce the probability of insider attacks.

Preventing insider threat requires removing or reducing the capabilities or factors that facilitate launching insider attacks. Adopting strong authentication techniques, strong passwords, laptop theft tracking decreases the probability of insider identity theft. Moreover, preventing employees from downloading or printing emails help in preventing insider threat.

SANS survey (SANS Institute, 2015) showed some factors that may limit preventing insider threat. Lack of training, lack of budget, lack of internal staff, lack of technology solutions are examples of these limitations. They survey demonstrated the most important tools and technologies used to prevent or deter insider threat. These tools are as follows.

- Content Filtering and Sandboxing of executables
- Inbound and outbound proxies
- Web filtering and content blocking
- Data Loss Prevention (DLP) with data flow analysis
- Data classification
- Net flow analysis to detect data exfiltration
- SIEM systems or other log-focused tools for detecting anomalies in user patterns
- User activity monitoring

Using these tools and technologies may reduce the risk of insider threat. However, advanced insider attacks may bypass these tools. Thus, implementing another level of security in insider threat mitigation is compulsory. Insider threat detection phase form the second layer that should by adopted by organization, especially banks, to mitigate insider threat.

Insider Threat Detection

Prevention controls do not always succeed in preventing insider attacks. Therefore, detection controls are needed to defend systems against insider threat. Auditing activities of insiders, especially accountants and managers, is a very crucial job in insider threat detection process. Most insider attacks were discovered during normal auditing activities.

Technical solutions must be correctly designed, implemented and configured to detect insider threat. According to the SANS survey (SANS Institute, 2015), the following solutions lead the pack for potential tools in insider threat detection.

- Internal audits
- Internal network monitoring
- Centralized log management
- SIEM tools
- External monitoring
- Employee monitoring
- Data Loss Prevention (DLP)

Most insider threat incidents were discovered during normal auditing activities. Therefore, checking log files and the activities of insiders are crucial in insider threat detection. Building patterns of insider threat incidents and using them for early threat alerting help in detection insider attacks in early stages. For example, some insiders follow specific steps when they intend to attack the banking system. These steps form a pattern of that kind of attack. Therefore, monitoring insiders' activities and checking them against this pattern (or a database of patterns in general), enable security officers to shed light on potential malicious insiders and stop them before the damage becomes sever. Hence, technical details behind these solutions are behind the scope of this chapter.

Damage Assessment and Recovery

Insiders can cause huge loss in banking systems due to the expensive value that this sector has. Financial loss is the major loss that banking sector suffers. However, bank reputation and reliability are major elements that may be harmed by insider threat. Reducing the damage caused by insider threat starts by early detection of attacks and fast assessment and recovery. Training incident response team is a major step towards having rapid assessment and recovery after insider attacks. Creating attack models to train and evaluate the incident response team may help in reducing the losses after attacks. Moreover, implementing secure backup and recovery processes, and testing them periodically is crucial in fast recovery.

SUMMARY

Insider threat is a major concern in banking sector. According to many surveys, the losses that are caused by an insider are greatly more than the losses caused by a hacker. Despite the aforementioned fact, banks still invest much more money in mitigating outsider attacks than mitigating insider threat. Therefore, banks should pay more attention to this threat, and should invest more money in developing tools to mitigate this threat.

The insider threat cases that have been discussed in this chapter shows that insiders may launch different types of attacks, such as technical and non-technical attacks, attacks on banking systems and attacks on the Personally Identifiable Information (PII). The later type of attacks is the most common one in insider threat in banking systems. Therefore, banks should pay more attention to the PII, and limit the access to this important information using high secure access controls, and implementing good auditing and monitoring tools.

Securing banking systems may not guarantee the block of insider threat door. However, multiple levels of security help in greatly reducing the probability of insider attacks. Good tools and security policies should be used to prevent insider threat. However, advanced insider attacks that succeed in bypassing insider threat prevention tools should be detected. Adopting reliable insider threat detection countermeasures is crucial in reducing the damage caused by malicious insiders. Moreover, training incident response team about fast assessment and recovery after attacks is very important in controlling the insider attacks and reducing the damage.

REFERENCES

Brackney, R., & Anderson, R. (2004). *Understanding the insider threat(technical report)*.Santa Monica, CA, USA: RAND Corporation.

Cappelli, D., Moore, A., & Trzeciak, R. (2012). *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. Addison-Wesley Professional.

CERT. (2011). *The 2011 CyberSecurity Watch Survey*. Retrieved from www.cert.org/

Childs, M. (2013). *JPMorgan Whale Pushed for 'Young' Trader Who Later Took His Job*. Retrieved from http://www.bloomberg.com/news/articles/2013-03-18/jpmorgan-s-whale-advocated-young-trader-who-later-took-his-job

Cooper, R. (2008). *Verizon Business Data Breach Security Blog*. Retrieved from http://www.securityblog.verizonbusiness.com/2008/

Cummings, A., Lewellen, T., McIntire, D., Moore, A., & Trzeciak, R. (2012). *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector* (Special Report CMU/SEI-2012-SR-004). CERT Program. Retrieved from www.sei.cmu.edu/reports/12sr004.pdf

Cuomo, A., & Lawsky, B. (2014). *Report on Cyber Security in the Banking Sector*, New York State Department of Financial Services. Retrieved from http://www.dfs.ny.gov/reportpub/dfs_cyber_banking_report_052014.pdf

Forrester Research. (2010). *The Value of Corporate Secrets*. Retrieved from https://www.nsi.org/pdf/reports/The%20Value%20of%20Corporate%20Secrets.pdf

Gordon, L., Loeb, M., Lucyshyn, W., & Richardson, R. (2005). *Computer Crime and Security Survey*. Retrieved from http://www.cpppe.umd.edu/

InfoSecurity Europe. (2010). *Information Security Breaches Survey*. Retrieved from http://www.pwc.co.uk/eng/publications/isbs survey 2010.html

Mario, S. (2013). *17 Proven Currency Trading Strategies: How to Profit in the Forex Market*. Wiley.

Richards, K. (2013). *FBI Offers Lessons Learned on Insider Threat Detection*. Retrieved from http://searchsecurity.techtarget.com/news/2240179082/RSA-2013-FBI-offers-lessons-learned-on-insider-threat-detection

Richardson, R. (2010). *15th Annual 2010/2011 Computer Crime and Security Survey*. Retrieved from http://gatton.uky.edu/faculty/payne/acc324/CSISurvey2010.pdf

SANS Institute. (2015). *Insider Threats and the Need for Fast and Directed Response, A SANS Survey*. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/insider-threats-fast-directed-response-35892

Subashini, S., & Kavitha, V. (2010). A Survey on Security Issues in Service Delivery Models of Cloud Computing. *Journal of Network and Computer Applications*, *34*(1), 1–11. doi:10.1016/j.jnca.2010.07.006

United States Government Accountability Office USGA. (2015). *Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information*. Report to Congressional Requesters. Retrieved from http://www.gao.gov/assets/680/671105.pdf

Walker, P. (2012). UBS rogue trader Kweku Adoboli jailed over 'UK's biggest fraud'. *The Guardian.* Retrieved from http://www.theguardian.com/uk/2012/nov/20/ubs-trader-kweku-adoboli-jailed-fraud

Wang, J., Gupta, M., & Raghav, H. (2015). Insider Threat in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications. *Journal of MIS Quarterly*, *39*(1), 91–112.

Yaseen, Q., & Panda, B. (2009). Knowledge Acquisition and Insider Threat Prediction in Relational Database Systems.*Proceedings of the 2009 International Conference on Computational Science and Engineering*, Vancouver, Canada. doi:10.1109/CSE.2009.159

Yaseen, Q., & Panda, B. (2012). Insider Threat Mitigation: Preventing Unauthorized Knowledge Acquisition. *International Journal of Information Security, 11*(4), 269–280. doi:10.1007/s10207-012-0165-6