Segregation-of-duties conflicts in the insider threat landscape

An overview and case study

Sherwin Ballesteros
Deakin University,Melbourne. Australia
sballest@deakin.edu.au

Lei Pan
Deakin University, Melbourne. Australia
l.pan@deakin.edu.au

Lynn Batten
Deakin University, Melbourne. Australia
lmbatten@deakin.edu.au

Gang Li
Deakin University, Melbourne. Australia
gang.li@deakin.edu.au

Abstract - **Many insider attacks originate from misuse of privileges granted by organizations to their internal employees, contractors or third-party service providers. A fundamental means of ensuring that conflicts of privilege cannot occur is to segregate role allocations in order to ensure that no individual can perform a task from beginning to end. In this paper, we provide background on insider attacks in connection with conflicts in Segregation of Duties, and present the current strategies for preventing and detecting such conflicts. To illustrate how a conflict can occur and what can result, we present an in-depth case study demonstrating a conflict in Segregation of Dutiesin an organization, along with the consequent fraud, and we discuss how it might have been prevented.**

Keywords-insider threats; segregation-of-duties; SoD; misuse of privileges

I. SEGREGATION OF DUTIES AND INSIDER THREATS

Cyber-attacks are a challenge to many organizations for whom network connectivity is a major support to the business. Cyber threats come from organized crime units who specifically target certain organizations, as well as from opportunistic individuals including contractors and internal employees. Regardless of the threat source, these attacks have implications for the organizations targeted, including the waste of valuable time in conducting security investigations and forensic analysis, in recovering from successful intrusions and in addressing subsequent regulatory implications. There is also the potential for damage to reputation and loss of shareholder trust.

For the purposes of this paper, we consider an ‘insider’ of an organization to be a person who has somelevel of access to the IT systems of the organization. Insiders are usually employees, contractors, consultants or personnel from third-party service providers who would have been granted legitimate access to IT systems [1]. An insider threat could arise from anyone in these categories because these people have knowledge of the internal IT system and sometimes of the security controls protecting it[2][3].

In many cases of insider-generated cyber-attacks, the perpetrator is someone already known to the organization. According to a global survey of over 10,000 senior company members located in the Americas, Europe, Africa, the Middle East and the Asia-Pacific regions conducted by PricewaterhouseCoopers in 2003 [4], current and former employees remain the highest internal threat source.

Results of the survey demonstrate that attacks originating from the internal network often develop from misuse of user privileges that have been granted to internal employees. In fact, the 2012 annual Data Breach Investigations Report by Verizon [5]highlighted that although the trend of insider attacks on organizations was decreasing, one of the main sources of breaches is from “abuse of system access privileges”.

The survey results demonstrate that one of the major challenges many organizations face is controlling who has access to fundamental systems and applications and allocating appropriate privileges to people to support them in performing their duties.

Segregation-of-duties **(SoD)** is a type of internal control many organizations implement to minimize the risk of fraudulent activities. It is designed to reduce the opportunity for fraudulent activities [6][7]. When properly implemented, it ensures that no individual can complete a critical business process from start to finish. It is also designed to ensure that users cannot execute multiple transactions resulting in conflict from a SOD standpoint, such as allowing a user to create a fictitious or fraudulent entry using one transaction, and the same user to conceal the fraud using another transaction [8].

According to Ernst & Young[7], the key reasons for SoD breaches include: (1) complexity and variety of the systems to implement it, (2) lack of ownership and accountability for controlling the processes, and (3) lack of proper checks and balances.

In the next section, we explore the current prevention and detection mechanisms designed to address the issue with SoD conflicts. This is followed by a case study describing how a breach of SoD enables an insider to attack a company, accompanied by discussion of what happened and how it could have been avoided.

II. Current Strategies for Prevention and Detection of SoD Conflicts

In this section, we explore the current prevention and detection mechanisms designed to address SoD conflicts.

A. Adoption of Industry-accepted Security Management Framework

A widely accepted approach is the adoption of good practices in information security management. ISO 27001 (based on the earlier version, ISO 17799) is the dominant security standard used by many organizations in information security management. This standard has a set of security controls designed to address the risk to information and information systems security.

B. Use of Deliberate Markers

It was noted by Schultz [1] that little progress has been made in regards to stopping internal attackers. Schultz attributed this problem to the lack of substantial understanding of the 'insider threat' [1]. In Schultz's paper, he indicated that what might be a promising approach in detecting and predicting insider attacks is the use of multiple regression techniques, utilizing a combination of behavioral and psychological attributes such as deliberate markers, meaningful errors, preparatory behaviors, verbal behaviors, correlated usage, and personality traits.

C. Implement an Audit System

King and Parulekar in their paper in 2004 [9] stated the need for an audit system that would enable an enterprise to determine a comprehensive set of incompatible functions. This was in response to the prominent corporate scandals surrounding the 2002 period. In their paper in 2004, King and Parulekar discussed an audit system, designed for segregation-of-duties reporting. This audit system could also verify the validity of segregation of incompatible functions, generate alerts when incompatible functions are assigned to the same individual, and further prevent access to incompatible functions.

D. Synergies between Technical And Procedural Processes, and Use of Neural And Statistical Methods

David [8] proposed a method based on Enterprise Planning Systems that would use a combination of procedural and technical processes to detect fraud. The paper [10] offered a comparison between utilizing neural networks and Bayesian methods in computer-related fraud detection.

E. Addressing SoD in ERP Systems

Proctor, Heiser, and MacDonald[11] discussed the following three techniques to address SoD conflicts in ERP systems: identifying and reducing conflicts at the application-level using functional permissions; integration with existing user provisioning and role management processes; automatically monitoring for transactions that indicate inappropriate behaviour.

F. Use behavioral Attributes to Tag Individuals

Although most current approaches in detecting insider threats are technical in nature, [12] argued that individuals with certain attributes are more likely to commit fraud than people who do not possess these attributes, and suggested to supplement technology-related controls with behavioral attributes and utilize personal background information by assigning 'tags' to internal employees which could include information about their financial, credit and bankruptcy history. The authors of [13] augmented this idea by proposing the addition of psychological attributes of people. In addition, it was suggested in[14] that behavioral and sociological aspects be considered to strengthen the defenses against insider attacks.

G. Audit Reporting

Many companies rely on audit reporting, where management is trained to use a software package that generates reports of conflicting duties [15]. The software packages available today, although preventive in nature, also have detection capability in the form of reporting. Reporting is manually invoked, and is usually performed at given time intervals, thus, this model does not provide for real-time detection of SoD conflicts.

III. ABS Banking Coporation – A Case Study on SoD Conflicts

A survey conducted by Gramling, Hermanson, Hermanson, and Yeregarding the nature of SoD weaknesses highlighted that the most common areas in accounting affected by the lack of SoD include cash disbursements, cash accounts, payables and receivables, purchase, and period-end closing [16].

The following case study illustrates how a SoD conflict was used to commit fraud during the purchasing process.

A. Company Background

ABS Banking Corporation(ABS) is a small-sized financial institution operating in the South East Asia region consisting of over500 employees.To assist operational management in purchasing any resource required to support its function, ABS uses a centralized purchasing IT system that is located in its headquarters in Singapore.

B. ABS' Purchasing Process

The purchasingprocess at ABS is composed of 8 key phasesand has defined rules (see Table 1) that must be followed when provisioning users to create a purchase order. This rule matrix is designed to minimize the risk of employee errors or deliberate and unauthorized transactions when processing purchase orders. The tasks which are marked 'X' mean they are conflicting duties. Therefore, users must not be assigned both of the corresponding tasks. This approach is aligned with [9] in which a list of incompatible functions is maintained.

The standard process for buying goods or services by employees on behalf of ABS Banking Corporation is illustrated in Figure 1.

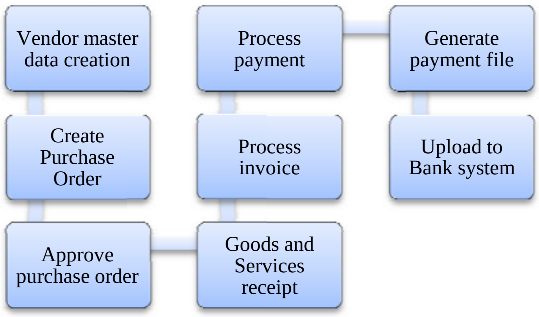

FIGURE 1. KEY PHASESIN THE PROCUREMENT PROCESS

If a vendor does not exist in the system, a user creates a record of the vendor in the database, including banking details for payment (*vendor data*).Once a purchase has been requested, a user *creates a Purchase Order (PO)* in the system. Before the request is further processed, an *approval of PO* is required. It is only at this point when the service or goods may be purchased. Once the *service or goods is received by ABS*, an *invoice is created and processed* for payment. Once the invoice has been processed, the vendor's *payment is now processed*, and a *payment file is generated*. This payment file is then uploaded to the Banking system (usually an application owned and hosted by a Bank).

C. The SoD Conflict at ABS Banking Corporation

To facilitate the procurement process, ABS setup the Procurement team. The team consists of 5 financial analysts, and is currently managed by Erica.Each of Erica's team members is tasked to perform certain activities throughout the procurement process e.g. maintain vendor data, create PO, approve PO, etc. One of Erica's team members, Vince, started with ABS 5 years ago as a Senior Financial Analyst. His tasks include the following:

- Receiving Goods and Services;
- Creating of Purchase Orders; and
- Generating payment files.

During Vince'sannual performance evaluation, Vince got good marks, however he did not get the promotion and pay rise he was expecting. As a result, Vince was unhappy with how the performance evaluation went and thought that the company was not rewarding employees according to their performance. Instead of getting the promotion he was expecting, Vince was given additional responsibilities, and is now tasked to do the following additional roles:

- Vendor master data creation; and
- Approving Purchase Orders.

The recent changes to Vince's role requiredmodification to his current user privileges. Provisioning of new user accounts is performed by ABS' IT department with approval from Erica for account creation or modification.

Vince knows the procurement process very well having been with ABS for 5 years. With the recent changes to his role, Vince noticed that he now has the capability to 'create' vendor data, and 'create' and 'approve' purchase orders. Vince saw this as an opportunity for revenge, and one day during normal business hours he entered a fictitious vendor called 'Com Tech' into the vendor master data. He listed Com Tech as an IT company providing IT consumables such as printer inks, toners, etc.and added his personal banking details to the system as Com Tech. After the vendor had been created, Vince then created a purchase order from it, which he subsequently approved. Because Vince also has the 'goods and services receipt' privilege, Vince knew that he would be able to falsify the receipt of any goods received from Com Tech.

After ABS processed the payment to Com Tech, Vince was able to collect funds from ABS through his fictitious vendor.

However, during ABS' annual audit of financial reporting systems, the external auditor noticed conflicts in roles assigned to certain employees, in particular, with Vince's user privileges. Following up on each identified case of lack of SoD, the auditor performed functional testing, where certain transactions during the year were sampled for details and tested for authenticity. During this test, it was determined that certain transactions with a vendor named Com Tech were both created and approved by Vince.Vince was challenged with this, admitted guilt and was dismissed from his position with the company.

IV. DISCUSSION

Many organizations adopt ISO27001 to form their information security management system. When properly implemented, the standard specifies setting up security governance and risk managementfunctions in an organization.Although the standard does not facilitate identifying conflicting roles for particular business processes (e.g. ABS' purchasing process), it forms a good baseline for security management.

The ISO standard supports regular auditing of reporting systems and therefore assisted in detecting Vince's fraudulent actwhich took place in our case study. This approach is also aligned with [9], and could be facilitated by a software package (used by ABS) as in [15] to perform audit reporting. The draw-back of this kind of audit is that it determines problems once they have happened. Detecting the likelihood of fraud in advance is more difficult.

The use of individual behavior profiling mentioned in parts B and F of Section 11, along with references [1], [12], [13], and [14]could be useful in identifying attributes of people who should be considered potential insider threats. However, the use of these attributesto tag an individual could result in challenges with regards to the privacy of the individual, which ABS would have to consider as a risk.

In the case of ABS andthe response to Vince's performance evaluation, Erica had several options. One of these was to analyze the components of Vince's proposed role allocation using the methods described in part D of Section II and discussed in papers [8] and [10]. However, there is no indication in the literature that the use of neural and Bayesian methods in [8] and [10], have been implemented to detect SoD conflicts.

An alternative method for Erica was to have created and implemented a role-matrix specifically for Vince's proposed roles similar to the example in Table 1.This matrix is the standard ABS matrix used in assigning roles in order to avoid SoD and Erica was at fault in not implementing it in this case.

To summarize, despite the threat being around for a number of years, proactively addressing incidents brought by a breach of SoD is still a significant challenge. Even with theavailability of commercial software packages,many organizations still struggle to effectively address SoD conflicts.

TABLE 1. EXAMPLE SOD ROLE-MATRIX

Process	**Create master data**	**Create PO**	**Approve PO**	**Receive Goods and Services**	**Process invoice**	**Process payment**	**Generate payment file**
Create master data		X	X	X	X	X	X
Create PO			X		X	X	
Approve PO		X			X	X	
Receive Goods and Services							
Process invoice						X	
Process payment		X	X		X		
Generate payment file		X	X				

V. FUTURE WORK

In this paper, we discussed some of the current strategies available to prevent and detect SoD conflicts, and have illustrated the challenges through a case study.

Fundamental to preventing and detecting insider attacks can be determining the motivation behind them. Hunker and Probst noted that this seems to vary among countries or geographic location [2]. In future work, we will continue to understand further the motivation behind fraud based on SoD conflicts, and explore ways of using behavioral or psychological attributes to identify potential insider threats.

REFERENCES

[1] Schultz, E.E., *A framework for understanding and predicting insider attacks.* Computers & Security, 2002. **21**(6): p. 526-531.

[2] Hunker, J. and C.W. Probst, *Insiders and insider threats—an overview of definitions and mitigation techniques.* Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2011. **2**(1): p. 4-27.

[3] Chivers, H., et al., *Knowing who to watch: Identifying attackers whose actions are hidden within false alarms and background noise. Information* Systems Frontiers, 2010: p. 1-18.

[4] PricewaterhouseCoopers *State of Global Information Security Survey (2013).* 2013. 37.

[5] Verizon *2012 Data Breach Investigations Report*. 2012. 76.

[6] Chong, G., *Detecting Fraud: What Are Auditors' Responsibilities?* Journal of Corporate Accounting & Finance, 2013. **24**(2): p. 47-53.

[7] Ernst_&_*Young A risk-based approach to segregation of duties*. 2010.

[8] David *Hendrawirawan*, H.T., Carl Zetterlund, Hunaid Hakam, Hyun Ho Kim, Hyewon Paik, CPA, and Yeohoon Yoon, *ERP Security and Segregation of Duties Audit: A Framework for Building an Automated Solution.* INFORMATION SYSTEMS CONTROL JOURNAL, 2007. **2**: p. 4.

[9] King, N. and Y. *Parulekar*, *Segregation of duties reporting*. 2004, Google Patents.

[10] Alford, M. *Intelligent fraud detection: a comparison of neural and Bayesian methods*. Computer Fraud & Security, 2013. **2013**, 14-16.

[11] Proctor, P.E., J. Heiser, and N. MacDonald, *MarketScope for Segregation of Duties Controls Within ERP, 2007.* R2183, 2007. **5222007**.

[12] Callahan, C.J., *Security information and event management tools and insider threat detection*. 2013, B.B.A, Gonzaga University: Monterey, California: Naval Postgraduate School. p. 102.

[13] Axelrad, E.T., et al., *A Bayesian Network Model for Predicting Insider Threats.* IEEE Security and Privacy Workshops, 2013: p. 8.

[14] Theoharidou, M., et al., *The insider threat to information systems and the effectiveness of ISO17799.* Computers & Security, 2005. **24**(6): p. 472-484.

[15] Changchit, C. and C.W. Holsapple, *The development of an expert system for managerial evaluation of internal controls.* Intelligent Systems in Accounting, Finance and Management, 2004. **12**(2): p. 103-120.

[16] Gramling, A.A., et al., *Addressing Problems with the Segregation of Duties in Smaller Companies.* 2010.