Presented at the DLSU Research Congress 2016
De La Salle University, Manila, Philippines
March 7-9, 2016

Framework to apply Risk based approach to Identity and Access Management (IAM) to address Negligent Insider in the BPO Industry

Merrynol L. Vasquez and Danny Cheng

College of Computer Studies, De La Salle University
**Corresponding Author: applevasquez@gmail.com*

Abstract: The growth of the BPO Industry has been significant in the past 10 years. Compared to other ASEAN countries, Philippines is the most trusted. It is projected to create 1.3 Million Jobs by 2016 and is consistently attaining $25 Billion in yearly revenue. With this significant growth, ASEAN Integration will definitely have an impact in BPO. As this Industry provides commercial presence in providing services to foreign owned companies, ASEAN Integration will open the possibility of the Philippines to become a BPO hub for South East Asia. This means that ASEAN members can freely work in the Philippines should a skill be needed such as skills that will involve their native language. These changes and challenges in adopting to cross cultural barriers also equates to Negligent Insider Risk which an organization must consider in preparing for the ASEAN Integration.

Negligent Insider Risk is an important factor since it is at the top list of the biggest Infrastructure threat having 55% of data breach. The chosen test bed for this research is the IT-BPO Industry. It is chosen due to its high turnover rate which increases the chance that a negligent act will be committed. Risk based IAM Framework of Forrester Research is the chosen Framework in this study. This risk based IAM Framework was created in 2014 and the risk application is based on the application being used. Since the research is about mitigation of Negligent Insider, the researcher will create guidelines to supplement the existing framework.

As an output, the research will formulate guidelines based on the principles of Risk Management. These guidelines will seek to mitigate Negligence in accessing company data in the BPO Industry.

Key Words: Identity and Access Management; Risk Management; Negligent Insider; Security; IT-BPO

1. INTRODUCTION

1.1 Negligent Insider

Insider Threat is considered as the most significant challenge facing Information Technology (IT) and security practitioners (Mills, et.al. 2011). One form of Insider Threat and is considered as a top infrastructure threat is Negligent Insider. It is simply an accidental harm on the data or system due to carelessness. As simple as it sounds, its effect is more damaging as expected. This acts of negligence can cause an organization to loose valuable data, serious risks to public and national security; disruption of operations which can eventually lead to financial loss or much worst, bankruptcy.

1.2 Business Process Outsourcing

Outsourcing has become a global phenomenon as organization hires a third party to handle a business process. It is a cost-saving strategy which is why organizations from USA and Australia opted to outsource their business function. Business Process Outsourcing or BPO is an industry susceptible to be affected by Negligent Insider Risk. It is a growing industry which ASEAN country is seeking to adopt.

The Philippines competes with other Asian countries in providing labor and infrastructure in the BPO Industry (Alava, 2006). Attrition is a threatening disease that has been surfacing in the Philippine BPO Industry as reduction in workforce takes place due to resignation, retirement and death (Anand, et.al. 2012). In a study by Business Mirror (2012), attrition rate in the Philippines runs up to 18%. This is like sighting that in every 100,000 workers, there are 18,000 incidents which are counted as attrition.

1.3 Risk based Identity and Access Management (IAM) Framework

Identity and Access Management or IAM is a high priority investment and a foundation in today's ICT enabled business models (Aberdeen Group, 2007). It is a *"security discipline that enables the right individuals to access the right resources at the right time for the right reason. "*(Gartner, 2014).

In 2014, Forrester Research released its Risk based IAM Framework. Within the framework are 10 Process which an organization have from the On-boarding up to termination or resignation of an employee. In every process, risk based IAM Framework is applied on the application being used by employees.

As mentioned, the framework is Risk based therefore it used the principles of Risk Management which are Risk Assessment, Risk Treatment, and Risk Monitoring. This framework by Forrester Research will be used in this study. Instead of focusing on the application being used, the focus is on applying principles of Risk Management to mitigate negligence in accessing data.

1.4 Relevant Literature

It is hard to create a standard profile on whether a person is negligent or not since a person can deny his negligence. Every type of Insider Threat looks the same but the way it was done and its intention varies. Monir (2010), a Chief Justice in India, published a book which explains how to understand the evidence as presented. Through understanding the evidence, the organization can be able to determine if an act is caused by negligence or not.

In an organizational set-up, it is not enough to know how to understand the evidence. There are policies being implemented to serve as access controls. However, the area of Negligence is not much emphasize to the controls that is why data consistently highlight Negligence as the "biggest infrastructure threat." IAM is seen as a solution on this problem since it optimizes business process. In 2007, Deloitte named four business drivers of IAM and one of this is Risk Management.

Incorporating Risk Management in IAM allows an organization to include strong audit trail and authentication, policy based compliance, and audit management. In this way, chances of mitigating Negligent Insider actions are made possible. For this reason, Forrester Research (2011) tagged IAM as a top security issue and a critical component of corporate security strategies. In fact, it is considered as a foundational element of any information security program (Ernst & Young, 2013). This shows that IAM is very important in an organization.

1.5 Scope and Objectives

BPO as a whole provides services to different sectors such as IT, education, healthcare, etc. In scoping this study, the focus is in the IT-BPO Industry which consist of sub-sectors namely: Back-Office, Knowledge Process Outsourcing (KPO), Software Design and Engineering, Animation, Game Development, Transcription and Call Center. Therefore, this study will not be specific to a company.

There are different types of Insider Threat and the focus will be on Negligent Insider particularly on Operational Risk which is the risk of daily business operations due to internal factors (people, process, system). Under these internal factors, the study will be specific to the identification and accessing of data.

The study will use Risk based IAM Framework of Forrester Research and will ensure that the created guidelines will supplement the existing framework.

Data validation will be conducted through Literature, Case Study, Interview and Focus Group Discussion to Subject Matter Experts. If ever there will be participants that will come from other industry, the researcher will ensure that their participation is chosen based on experience and that the information they will contribute is viewed in general, regardless of Industry. Participants from the IT-BPO Industry will be highly prioritized.

The objective of this study is to create Risk Management guidelines for the BPO Industry that will address Negligent Insider in the risk based IAM Framework of Forrester Research. The guideline will be based on the Risk Management process namely Risk Assessment, Risk Treatment and Risk Monitoring. Among the guidelines that will be created is related to Identifying Risk Indicator, defining Risk Levels, choosing a Risk Owner, constructing guidelines on when mitigation is done, how it is done and what are the controls; including gathering incident report/audit findings.

2. METHODOLOGY

The true impact of Negligent Insider can be known through understanding Risk. To fully understand how Negligent Insider can be mitigated, Risk Management will be the method in this study. The Risk formula is known as:

$$L \times I = R \qquad \text{(Eq. 1)}$$

where:

L = Likelihood
I = Impact
R = Risk

In the Risk equation, Likelihood is measured by the likelihood of an attack and the likelihood of the success of an attack. For impact, it can be measured through the impact when Negligence affects Confidentiality, Integrity and/or Availability (CIA).

There are four phases of Risk Management according to Gewald & Heinz (2004). These are:

1. Identification. Recognizing the sources of risk
2. Measurement. Estimating probabilities, severity, etc. to quantify risk
3. Management. Deciding on the appropriate action plan to handle risk
4. Control. Testing the success of measures taken to mitigate risk

In order for a risk to be solve, it is important to identify the Risk first. The first part of the guideline is about knowing the "signs" to look for that will tell if an individual is Negligent. This includes questions such as why is the act of negligence being done, what are the threshold that will tell that it is indeed negligent, etc.

Upon Identifying Risk, Assessment will follow. In assessing, the guideline will provide detailed checklist on what to look for in examining the components of risk which is likelihood and impact.

ISSN 2449-3309

Likelihood can be in two forms: How likely will negligence be done and how likely that the negligent act will succeed. In the process of looking at likelihood, ways on how it will be measured will be discussed. In knowing the Impact, it is important to know its value. The guideline will provide determining factors or sources of data which can help measure how high or how low a risk is. Next to assessment is the guidelines that will discuss how to treat negligence and how it can be monitored.

As a whole, in creating the guidelines, all possibilities will be looked at and the research will provide a definition on when to do and not to do certain things in order to mitigate negligence.

3. RESULTS AND DISCUSSION

Negligent Insider is an unnoticed Risk in any organization. In 2010, Deloitte-NASCIO reported 55% of internal information breaches were traced from either malicious in negligent acts.

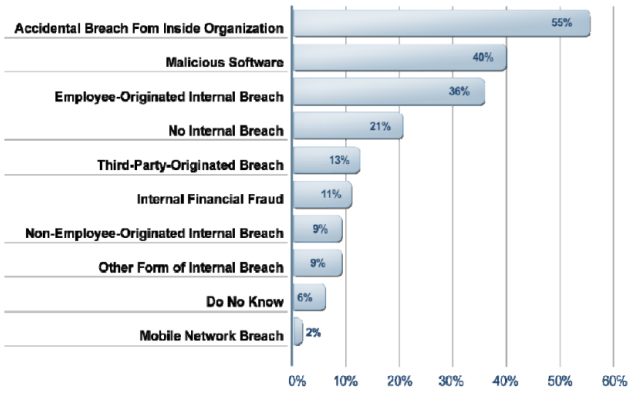

Fig. 1. Causes of Security Breach
(Deloitte and the National Association of State Chief Information Officers, 2010)

This claim was supported by a collaborative study by CERT Program, United States Secret Service's National Threat Assessment Center (NTAC), and Carnegie Mellon University (CMU). Their study shows that:

- 58% of insiders were employees with limited technical skills
- 54% of insiders was motivated by financial gain
- 85% of insiders had authorized access in the occurrence of malicious activity
- 69% is caused by access control gaps
- 22% of insiders attacked when business process or controls are weak. These can be due to poorly enforced policies and procedures in separation of duties

In the study mentioned, it is bothering to know that most of the insider breach were caused by people who are non-technical. If a non-technical person can breach data, how much more a technical person can cause damage to company information.

With the result of the above mentioned findings, it shows that there is an issue on how identity and access is provisioned to the users. Clearly, there is a big need to improve security without compromising business results.

In addressing these challenges, the goal is to create Risk Management based guidelines for the IT-BPO Industry that will mitigate Negligent Insider. These guidelines will ensure that it is accordance to the rules of confidentiality, integrity and availability of data within the organization. There are different reference materials in creating Risk Management, this research will use the work of Gewald & Heinz (2004).

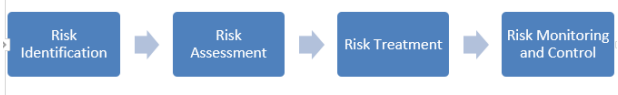

Fig. 2. Risk Management Phases
(Gewald & Heinz, 2004)

ISSN 2449-3309

4. CONCLUSIONS

In mitigating Negligent Insider, there is no such thing as "one solution fits all." Every organization has its own policies on how to mitigate. This research provides guidelines for each Risk Management process in order to mitigate Negligent Insider in the BPO Industry. The creation of guidelines will start from identifying signs of negligence. After which, assessment will be conducted wherein likelihood and impact will be detailed and measured. Risk Treatment and Monitoring will then follow.

The Potential Areas in this study is looking at negligence in a different industry or creating Risk Management guidelines for other Insider Threat such as Compromised Insider and Malicious Insider.

5. ACKNOWLEDGMENTS

The researcher would like to thank Mr. Danny Cheng, Thesis Adviser, for continuously providing knowledge and support to complete this research.

6. REFERENCES

Aberdeen Group (2007). Identity and Access Management Critical to Operations and Security. Communication News. Retrieved from: http://www.comnews.com/WhitePaper_Library/Managed_services/pdfs/Quest_Software_Aberdeen_IAM_Criical_to_Operations_and_Security.pdf.

Alava, A. (2006). Industry Report: The Problem of Sustainable Competitive Advantage in Philippine Call Centers. Philippine Management Review. Vol. 13, p. 1-20 Retrieved from: http://journals.upd.edu.ph/index.php/pmr/article/viewFile/1814/1725

Barkakati, L., (2005). How to do Risk Identification and Risk Mitigation. Paper presented at the Proceedings of the Knowledge Exchange Forum (U.S.). Retrieved from: https://www.pmiwdc.org/files/evt/kxf/RISK___Risk_Identification_and_Mitigation.pdf

Cross (2014). The Many Faces of Insider Threats. Retrieved from: http://insights.wired.com/profiles/blogs/the-many-faces-of-insider-threats#axzz3cRDeSEf0Report.

Deloitte-NASCIO (2010). State governments at risk: A call to secure citizen data and inspire public trust. The 2010 Deloitte-NASCIO Cyber Security Study. A Publication of Deloitte and the National Association of State Chief Information Officers [Online]. Retrieved from:http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_state_2010DeloitteNASCIOCybersecurityStudy_110910.pdf

Ernst & Young (2013). Identity and Access Management beyond Compliance. Insight on Governance, Risk and Compliance. Retrieved from: http://www.ey.com/Publication/vwLUAssets/Identity_and_access_management_-_Beyond_compliance/$FILE/Identity_and_access_management_Beyond_compliance_AU1638.pdf

Gartner (2014) Identity and Access Management Key Initiative Overview. Retrieved from: https://www.gartner.com/doc/2698426/identity-access-management-key-initiative

Hinz & Gewald (2004). A Framework for Classifying the Operational Risks of Outsourcing. Retrieved from: http://www.pacis-net.org/file/2004/S20-004.pdf

Mills, et.al. (2011). A Scenario-Based Approach in Mitigating Insider Threat. ISSA Journal. Retrieved from: http://www.dtic.mil/dtic/tr/fulltext/u2/a545628.pdf

Monir (2010). Textbook on the Law of Evidence. 8th Edition. Retrieved from: https://books.google.com.ph/books?id=ml3jDmdoU1gC&pg=PA75&lpg=PA75&dq=principles+on+how+to+know+if+act+is+intentional+or+unintentional&source=bl&ots=mK jY9-8xta&sig=GdmQtD1wDf3mNnSQQIit4VkhNB8&hl=en&sa=X&ei=XAhzVfHoAoHjoATo9oLYAg&redir_esc=y#v=onepage&q=principles%20on%20how%20to%20know%20if%20act%20is%20intentional%20or%20unintentional&f=false

OSF Global Services (2012). Mitigate BPO Security Issues. Retrieved from: http://www.osf-global.com/assets/uploaded_files/de/mitigate-bpo-security-issues-OSF-whitepaper.pdf