INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 8, Issue 10, (2018) E-ISSN: 2222-6990

A Review on Insider Threat Status in Malaysian Organization

Isnin, S.N.[1] & Sedek, M[2]

[1] Faculty of Technology Management and Technopreneurship, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

[2]Centre for Academics Excellence and Scholarship, Universiti Teknikal Malaysia Melaka Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v8-i10/5291 DOI:10.6007/IJARBSS/v8-i10/5291

Published Date: 03 October 2018

Abstract

An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems. The threat may involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property, or the sabotage of computer systems. Insider threat ranks among the most pressing cyber security challenges that threaten government and industry information infrastructures indirectly give the negatively impact to industries and national security. The threat that insiders pose faced by corporations and governments today is a real and significant problem and to be of serious concern. Selling and sharing confidential information industrial design, organisational strategic plans, customers, suppliers, experts and other valuable information for monetary benefit, revenge, bribery are just some of the examples of insider threats. many are familiar with the damage of insider threat but some of them are familiar with the terms of drudge, cyber plan of attack, cyber security system and others. Therefore, the purpose of this paper is to review issue related to insider threat, potential people to be insider threats, reasons to be an attacker, and the characteristics of the insider threat, as well as to seek more information on the impact to the organisation's performance. Therefore, it is hoped that this paper will assist readers, especially the top management of the organizations to understanding more on the issue related to the insider threat.

Keywords: Insider Threat, Cyber Security, Malaysian Organisation

Introduction

A globally-interconnected digital information and communication infrastructure, which may be referred to as "cyberspace" supports the functionally of almost every system in the modern world. Economic, transportation, communication, energy and security systems, among other systems, are highly reliant on information and communications

technology (ICT). Small business would be unable to continue their day-to-day operations without access to the current cyber infrastructure, and such a situation would be even more profound on Wall Street. ICT provides mechanisms for more efficient and convenient transfer of information than ever before; however, it also brings substantial risks. The retailer target believes as many as 70 million customers were affected by a data breach in late 2013; Home Depot estimated that up to 56 million credit cards may have been compromised in a 5-month-long breach in 2014 and approximately 76 million households and 7 million small business were affected by the cybersecurity breach at JP Morgan in the summer of 2014 (Hutchins et al. 2015).

Malaysia has high vulnerability to cyber attacks. Malaysia is regarded as one of the top ten countries that are vulnerable to cyber attack, besides the United States and North Korea. According of cyber security expert, he said 65 percent of organisations in Malaysia face risks of cyber attacks (Amiruddin**,** 2016). Cyber security Malaysia received more than 10 thousand reports and cases regarding to cyber attacks and crimes every year. Threats come from many part such as from the physical human, technology, system and so on. However, even though some of the threats come from the cyber or internet or a system there is an authorised people who need to control and maintain the program till success. Meaning here the big issues will start from the physical of the human itself is reality.

Nowadays, computers has become essential to corporate sectors and government organizations to move from conventional computing system to cyber system. Thus we can say that we all are surrounded and dependent on continued availability, confidentiality and accuracy of Information and Communication Technologies (Sedek, Ahmad, & Othman, 2018**;** Sedek, Mahmud & Daud, 2014). Attackers may use different technique to harm a particular organization in different ways. It impacts an organization in different ways like economically, business disruptions etc. There is no specific solution to attacks but the awareness and implementation of policies is the best suggestion to this growing era. (Yadav and Gour 2014). When the words of cyber attackers combined is can be define as the threats from a person who have their own technique to attack and harm or sabotage something by using the information technology such as internet, systems and others.

Most of the organisation have their own asset or confidential data and information that need to be protected. All the confidential data including details of the employees, documentation, design, financial and others. At this point of view, this information need to be protected from threat that comes from inside of the organisation and this is what we call it as insider threat if the threat is happen in the organisation.

Literature Review

Threat or danger or harm is an expression of an intention to inflict pain, harm, or punishment. Also can be called as an indication of impending. One that is regarded as a possible source of harm or danger, viewed the stranger as a threat to the community. The condition of being in danger or at risk: under threat of attack. In computer security, a threat is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm. A threat can be either intentional example hacking such as an individual cracker or a criminal organization or accidental example the possibility of a computer malfunctioning, or the possibility of a natural disaster such as an earthquake, a fire, or a tornado or otherwise a circumstance, capability, action, or event (Yadav & Shashant, 2014).

Employees or authorise person can compromise the security of an organisation with their overzealousness in getting their job done. Every organisation has a varied mix of employees, consultants, management, partners and complex infra-structure and that makes handling insider threats a daunting challenge. With insider attacks, organisations face potential damage through loss of revenue, loss of reputation, loss of intellectual property or even loss of human life attacks, organisations face potential damage through loss of revenue, loss of reputation, loss of intellectual property or even loss of human life. (Roy, 2010).

The terms insider threats and the risks associated to it are not new and strange to companies in Malaysia. But, most of these companies choose not to openly confront the risk and prefer to handle it in their subtle way. They are reluctant to state their experience and difficulties dealing with issues related to the insider threats. It was probably due to adverse reputation and fear if revealing the fact that trusted people within their organisation who commits wrongdoings or fraud will further contribute undesirable impact to the company's operations and customers' perception. Such incidents (insider attacks) could result in reputation loss to the affected organization (Apau, Sedek & Ahmad, 2018).

From Malaysian perspective, documented references such as literature review, journals, articles, books and such. of insider threats are scarcely found throughout this research journey. It was evidently showed via Scopus online search conducted in 05 January 2016. The "Insider Threat" was entered as the input keyword and produced 670 results of related document submissions from 52 different countries. The highest submission came from the United States of America (i.e. 51.1%) and followed by United Kingdom (i.e. 8.4%), China (i.e. 5.1%), Canada (i.e. 3.1%), Australia (i.e. 3.1%), South Korea (i.e. 2.8%), India (i.e. 2.6%), Germany (i.e. 2.3%) and Japan (i.e. 2%). Malaysia has contributed less than one percent (i.e. 0.5%) from the total submission.

In addition, from others documented references recorded by Cyber Security Malaysia and Cyber999 in Malaysia. It was showed from to 2011 there was increased a lot of percentage from time to time. In February, 2010 87% percent of all Malaysian web traffic is malware. From 2009 to 2010 there was increased from 3564 cases to 8090 cases. Total number of reported cyber crime in 2011 was 14157. This is hard evidence that shows cyber crimes are increasing at an alarming rate.

Figures and Tables

NO	AUTHORS	STATISTICS	STATEMENTS
1	Symantec's Internet security threat report 2010, February. Robin Hicks who attended as a speaker in a high level government, Cyber security Malaysia, 2010	1- 87 percent of all Malaysian web traffic is malware. Only 0.2 percent originated from Malaysia to global neteworks.	This issue of cyber security has been investigated by Robin Hicks - he stunned his audience of Malaysian civil servants when he showed a slide show with Malaysian government's website which was hacked and festooned with images of naked woman.
2	Lalitha Muniandy and Dr. Balakrishnan Muniandy	Increased 127 percent within 1 year period - Increased from 3564	

	Cyber Security Malaysia, 2010 Recorded by cyber 999 in Malaysia	cases in 2009 to 8090 cases in 2010	
3	Lalitha Muniandy and Dr. Balakrishnan Muniandy Cyber Security Malaysia, 2011 November According to Lt Col (Rtd) Prof Datuk Husin Jazri, The cyber security Malaysia chief executive officeer, 2011 August	Total number of reported cyber crime recorded was 14, 157.	This is hard evidence that shows cyber crimes are increasing at an alarming rate.
		10, 000 cases reported every month in Malaysia	He added that the Cyber Early Warning System that has been set up by Cyber security Malaysia detected over 5, 000, 000 security threats until August 2012. (Jo, Timboung, 2011)

Figure 1. The statistic threats in Malaysia 2010-2011

Based on the literature reviews conducted, there were many insider threats definitions found. For this study, the definition was from the Computer Emergency Response Team at Carnegie-Mellon University (CERT). It defines insider threat as “a malicious insider who is a current or former employee, contractor, or business partner who has or had authorized access to an organisation’s network, system or data, and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organisation’s information system” (Myers, Grimaila, and Mills 2009). The above definition was further explained by Bishop as, “when the trusted entity that is given power to violate one or more rules in given security policy” (Bishop, Position:Insider is Relative, 2013). He later defined that the insider threat can be further elaborated when violation of security policy using legitimate access, and violation of an access control policy by obtaining unauthorised access (Legg, 2011).

From the literature review, it has been found that the insider threat has been defined as current or former employee, contractor or other business partner who has or had authorised access to an organisation's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity or availability of the organisation's information or information system. (Clark, 2016).

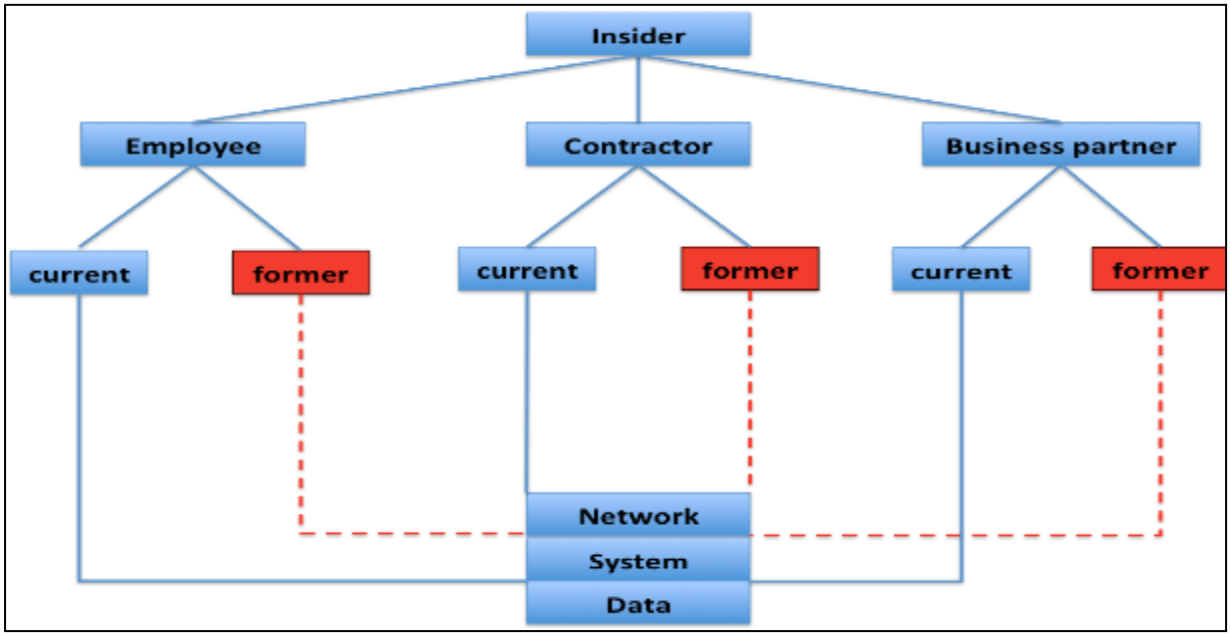

Figure 2. Insider threat definition
(Tuor, Kaplan, Hutchinson,Nichols, N., & Robinson, 2017).

Results and Findings

It can be explained as the threat that happen inside the organisation by the employees or one of their authorize person. Meanwhile according to Nurse et al., insider threat is individual party, who has privileged access to the networks, systems or data of an organisation (Nurse, 2014).

Insider threat involved three parties which are the employee, the contractor and the business partner from the (past or current). It can be consider two categories of insider threat. The first is a malicious insider threat, where the insider uses their privileged access to intentionally cause a negative impact to the confidentiality, integrity or availability of the network, systems and data.

In this paper we will consider categories type of insider threat which come from within by using the internet or system and one more from the human physical. However there is two types of attackers which is by an intentional misused meaning here that they be an attacker because of they want to cause a negative impact to the organisation. One more is by unintentional attackers which is they more to human mistakes or errors such as accidentally leaking sensitive company information on social networks (Tuor, Kaplan, Hutchinson, Nichols & Robinson, 2017).

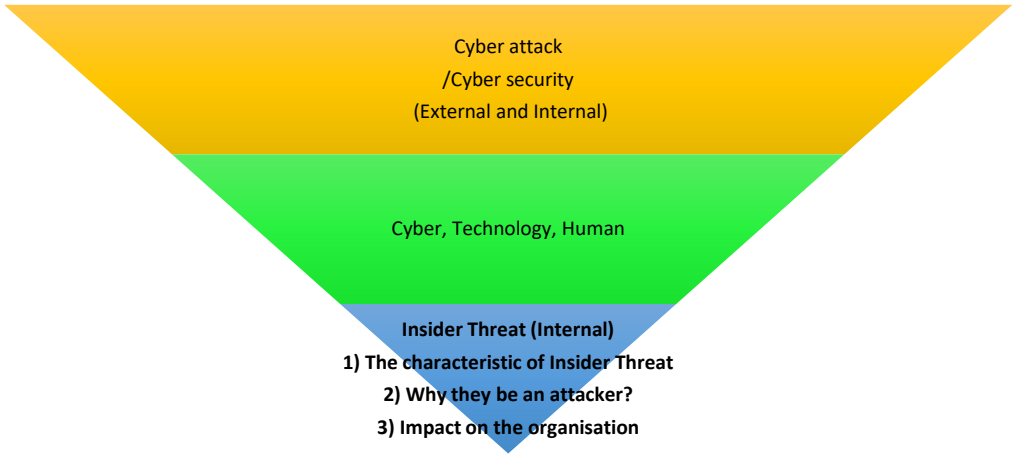

Figure 3. The illustration of the insider threat

Conclusion

As a conclusion, prevention of insider threats begins with employee education. Employees must be made to understand the potential consequences of risky behavior, such as password sharing and sharing of other sensitive information. Implementation of appropriate procedures when employees terminate their employment is also critically important to prevent former employees from being able to gain access to the system. For non-IT employees, this means immediately deleting or disabling user accounts. For IT employees, disabling a user account may not be enough; any administrative passwords throughout the IT infrastructure that a former employee had access to must also be changed. Behavioral monitoring is an important tool for detecting and mitigating insider threats. A former employee with malicious intent may attempt to access target systems remotely, outside of normal business hours or both. As such, it is important to audit and review failed remote login attempts, especially those that occur at odd times. Last but not least, to promote more effective mitigation of insider threats, it must address critical challenges in detecting, confirming, and integrating cyber and behavioral indicators of insider threat risk (Frank, Justin, et al 2018).

Acknowledgement

The researchers would like to express our gratitude to the Ministry of Higher Education (KPT) for sponsoring this study under the research grant RAGS/1/2014/1CT01/FPTT/B00076. We would also like to thank Universiti Teknikal Malaysia Melaka for the opportunities given to us during this project period.

References

Amiruddin, A. W. (2016), Cyber Security Malaysia. “Malaysia Has High Vurnerability To Cyber Attacks, Says Cyber Security Expert • UKM News Portal.” *UKM News Portal*. Retrieved (file:///C:/Users/USER/AppData/Local/Mendeley Ltd/Mendeley Desktop/Downloaded/Unknown - Unknown - Malaysia Has High Vurnerability To Cyber Attacks, Says Cyber Security Expert • UKM News Portal.html).

Apau, M. N., Sedek, M., & Ahmad, R. (2018). Inclination of Insider Threats’ Mitigation and Implementation: Concurrence View from Malaysian Employees. In International Conference on Knowledge Management in Organizations (pp. 340-352). Springer, Cham.

Clark, W. (2016). "Threat from Within: Case Studies of Insiders Who Committed Information Technology Sabotage." *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016* 414–22.

Hutchins, J. (2015). "Framework for Identifying Cybersecurity Risks in Manufacturing." *Procedia Manufacturing* 1:47–63. Retrieved (http://linkinghub.elsevier.com/retrieve/pii/S2351978915010604).

Legg, P. (2011). "Towards a Conceptual Model and Reasoning Structure for Insider Threat Detection." 4, (1-18).

Myers, J. & Grimaila, M. (2009). "Towards Insider Threat Detection Using Web Server Logs." *… of the 5th Annual Workshop on Cyber …* 1. Retrieved (http://portal.acm.org/citation.cfm?doid=1558607.1558670%5Cnhttp://dl.acm.org/citation.cfm?id=1558670).

Nurse, R. C. (2014). "Understanding Insider Threat: A Framework for Characterising Attacks." 1–16.

Roy, S. (2010). "Assessing Insider Threats to Information Security Using Technical, Behavioural and Organisational Measures." *Information Security Technical Report*.

Sedek, M., Ahmad, R., & Othman, N. F. (2018). Motivational Factors in Privacy Protection Behaviour Model for Social Networking. In MATEC Web of Conferences (Vol. 150, p. 05014). EDP Sciences.

Sedek, M., Mahmud, R., Jalil, H. A., & Daud, S. M. (2014). Factors influencing ubiquitous technology usage among engineering undergraduates: a confirmatory factor analysis. Middle-East Journal of Scientific Research, 19, 18-27.

Tuor, A., Kaplan, S., Hutchinson, B., Nichols, N., & Robinson, S. (2017). Deep learning for unsupervised insider threat detection in structured cybersecurity data streams. arXiv preprint arXiv:1710.00811.

Yadav, H. & Shashant, G. (2014). Cyber Attacks: An Impact on Economy to an Organization . *International Journal of Information & Computation Technology* 4(9):937–40. Retrieved (http://www.).