DOI link to article:

https://doi.org/10.1109/RCIS.2017.7956579

Date deposited:

29/08/2017

Security Threat Classification For Outsourced IT Projects

Moneef Almutairi
School of Computing Science
Newcastle University
Newcastle Upon Tyne, UK
moneef.almutairi@ncl.ac.uk

Stephen Riddle
School of Computing Science
Newcastle University
Newcastle Upon Tyne, UK
steve.riddle@ncl.ac.uk

Abstract— Many organisations have adopted outsourcing for delivering critical IT services to their clients. Organisations need to identify the potential security threats of outsourced IT projects as early as possible to avoid or mitigate security incidents. Existing threat classification approaches suffer from limitations such as the lack of exhaustive threat classification criteria. In this paper, we propose a threat classification approach for outsourced IT projects. This approach aims to allow organisations to identify, minimise, mitigate, or eliminate security threats at the early stages of project execution.

Keywords— threat classification approach, outsourced IT projects, outsourcing threat classification.

I. INTRODUCTION

With the increasing complexity of modern information systems, and organisations' need to refocus their resources on core business activities, many organisations adopt outsourcing as the principal means of delivering critical Information Technology (IT) services for themselves and their clients. Outsourcing is an attractive option for organisations, offering benefits including cost reduction and the opportunity to concentrate on core business activities. However, it is an option that must be managed properly as it brings risks such as compromised security, contract violations, and the loss of technology skills for the organisation [1]. Failure to manage such risks could lead to major issues not only in a particular project, but also for the entire organisation or business [2].

Identifying and analysing potential security threats at the early stages of a project's execution play a vital role in managing the security risks of outsourced IT projects. Threat identification should follow a systematic approach that is capable of capturing the wide range of threats that the project might face, as attackers may need only one security weakness to break the entire system [3].

II. BACKGROUND AND RELATED WORK

There have been several attempts at classifying threats to information systems in the literature. Those attempts can be classified into two main categories [4]:

A. Threat classification approaches based on attack techniques

In this type of threat classification, the techniques that are employed by attackers to exploit any system vulnerabilities are used to classify threats. Examples of this approach are the threat cube model [5], and the threat pyramid model [6].

This type of threat classification approach does not take into consideration the impact of the identified threats on information systems or asset identification and categorisation, which help an organisation to know what to protect and how. It is not appropriate for the outsourcing context, where threats arise from different agents such as providers, clients, external attackers, and environmental and physical threats.

B. Threat classification approaches based on attack impact

In this type of threat classification approach, the goals of attackers are used to classify threats. The Microsoft STRIDE model, and the ISO 7498-2 model [4] are examples of this approach.

This type of approach uses only one criterion, threat impact, for classifying threats. The fact that it does not use exhaustive criteria could decrease its ability to identify threats that might affect information systems. It does not provide a systematic approach that can help to identify a wide range of threats.

With the advancement in information technologies and distributed systems, as well as the involvement of different parties in managing particular information systems, the risk of threats has increased. In addition to the fact that the responsibility for managing security threats might be lost among those parties, existing threat classification approaches fail to address such risks properly. In the outsourcing context, where environments are less stable and more systems are integrated together, the threat classification approach therefore needs to possess certain desired properties to address potential security threats adequately. It should be exclusive, exhaustive, unambiguous, repeatable, comprehensive and useful to capture the largest possible number of potential security threats [4].

III. THREAT CLASSIFICATION FOR OUTSOURCED IT PROJECTS

We propose a new hybrid threat classification approach for the outsourcing context. The proposed approach combines different threat classification criteria and takes into consideration the desired properties that a good threat classification approach should have. It is a systematic approach that provides a comprehensive threats analysis and takes into account threats from different perspectives such as external threats, provider threats, client threats, and physical and environmental threats. Fig 1 shows our proposed threat classification for outsourced IT projects.

The threat classification criteria that we use in our proposed approach are described as follows:

- Threat Source: the origin of the threat, which can be external threats, client threats, provider threats, or environmental and physical threats.
- Threat agent: the agent that causes the threat. This can be technical, human, or organisational.
- Asset type: the type of the asset impacted by this threat. This can be networks, software, hardware, or information.
- Threat intention: the type of human behaviour that caused the threat. It can be accidental or intentional.
- Environmental and physical threat type: the type of environmental or physical threats. It can be controlled or non-controlled.
- Threat impact: the result of the threat on the information system. It can affect the confidentiality, integrity, or availability.

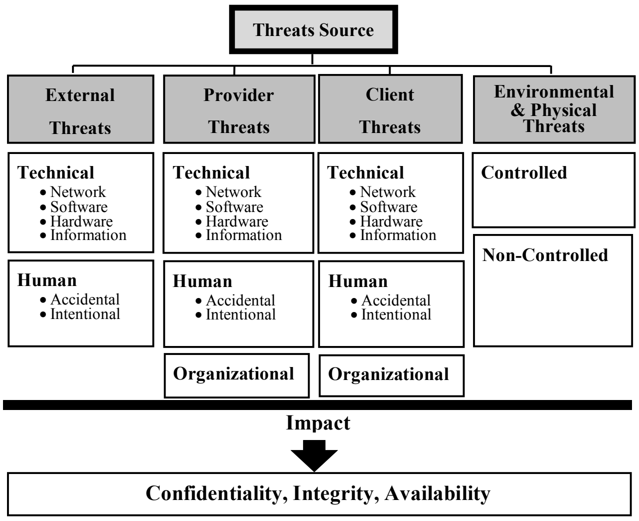

Fig 1: Outsourcing Threat Classification

In the outsourcing context, where different parties are involved in the project execution, we believe that the source of threats can be one of four: external attackers, the provider itself, the client, and environmental and physical threats.

External threats are either technical or human. Technical threats are those that target one or more of the project's or organisation's assets. They can target the network, software, hardware, or information assets. Such threats employ technology (e.g. the internet) to attack the project and organisational assets. Human threats might be accidental or intentional and they represent threats that are imposed by non-technical actions such as accessing buildings and collecting sensitive information without permission.

The provider threats category represents threats that are imposed by the provider who executes the project. Provider threats are divided into three categories: technical, human, and organisational. Technical threats represent threats that affect one or more of the project or organisational assets. They can affect the network, software, hardware, or information assets. Such threats use technology to affect the assets (e.g. software bugs). Human threats might be accidental or intentional and they represent threats that are imposed by non-technical actions such as accessing client data centres without permission and collecting sensitive information about the client. The organisational threats represent threats imposed by a lack of adequate security procedures and processes (e.g. lack of security policies), which might impose security threats on both the client and the provider.

The third category is client threats. This category has greater importance, especially when there is any type of integration with the client's existing systems. Such integration might affect the confidentiality, integrity or availability of the client's existing systems. The client threats contain the same categories as the provider threats. This category is designed to overcome the limitations of some existing threat classification approaches that do not take into consideration insider security threats.

The fourth category is environmental and physical threats. This category represents threats that arise from the environmental and physical conditions. These threats might be controlled, such as controlling the temperature of the data centre, or uncontrolled, such as earthquakes.

The results of any threat from any source could lead to major security risks to confidentiality, integrity, or availability.

IV. Conclusion

In this paper, we propose a threat classification approach for the context of outsourced IT projects. It is designed to possess all of the desired properties that a good threat classification approach should have. The proposed approach also overcomes the lack of exhaustive criteria limitation of existing threat classification approaches. It is designed to be a systematic and comprehensive approach that suits the outsourcing context, where different parties are involved in the project execution. Threats are considered from different perspectives to capture the largest possible number of potential security threats that the project might face. We aim to apply this approach to a real case study in the near future, and also to use a focus group to provide independent validation evidence.

References

[1] K. Han and S. Mithas, "Information Technology Outsourcing and Non-IT Operating Costs: An Empirical Investigation," *MIS Quarterly,* vol. 37, pp. 315-331, 2013.

[2] J. Iqbal, R. Binti Ahmad, and M. A. Noor, "Frequently occurring risks for IT outsourcing projects," *in International Conference on Computer and Communication Engineering (ICCCE),* pp. 957-960, 2012.

[3] S. Myagmar, A. J. Lee, and W. Yurcik, "Threat modeling as a basis for security requirements," in *Symposium on requirements engineering for information security (SREIS)*, pp. 1-8, 2005.

[4] M. Jouini, L. B. A. Rabai, and A. B. Aissa, "Classification of security threats in information systems," *Procedia Computer Science,* vol. 32, pp. 489-496, 2014.

[5] S. Gerić and Ž. Hutinski, "Information system security threats classifications," *Journal of Information and Organizational Sciences,* vol. 31, pp. 51-61, 2007.

[6] M. Alhabeeb, A. Almuhaideb, P. D. Le, and B. Srinivasan, "Information security threats classification pyramid," *in IEEE 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA),* pp. 208-213, 2010.