INFORMATION SECURITY IN DATA CENTRE

(GOVERNMENT ECO-SYSTEM)

SEEMA KHANNA

DEPARTMENT OF MANAGEMENT STUDIES

INDIAN INSTITUTE OF TECHNOLOGY DELHI

OCTOBER 2017

INFORMATION SECURITY IN DATA CENTRE

(GOVERNMENT ECO-SYSTEM)

by

SEEMA KHANNA

Department of Management Studies

Submitted

in fulfillment of the requirements of the degree of Doctor of Philosophy

Indian Institute of Technology Delhi

October 2017

Certificate

The thesis entitled "**Information Security in Data Centre (Government eco-system)**", being submitted by **Ms. Seema Khanna** to the Indian Institute of Technology Delhi, for the award of the degree of "**Doctor of Philosophy**" is a record bona fide research work carried out by her. She has worked under my supervision in conformity with rules and regulations of the Indian Institute of Technology Delhi. The research reports and results presented in the thesis have not been submitted in part or full for the award of any degree or diploma in any other University or Institutes**.**

Date:

Place:

Dr. Harish Chaudhry
Associate Professor
Department of Management Studies,
Indian Institute of Technology Delhi,
Hauz Khas New Delhi

Acknowledgements

First of all, I would like to thank my supervisor **Dr. Harish Chaudhry** for allowing me to work under his supervision. I am highly indebted to Dr. Chaudhry, who gave enough freedom to explore new things and cautioned me whenever I used to get distracted to other paths and always motivated me in my down times.

I am also thankful to faculty of DMS for their invaluable suggestions and critiques that helped me in reframing my research questions and presenting my work in a more decent format.

I would like to thank family who have been my real inspiration and always encouraged me for pursuing higher studies.

My friends & other PhD fellows in this journey, who cannot be forgotten for their unconditional support and encouragement. All my friends supported me in writing, and incented me to strive towards my goal. Their contributions cannot be compensated in any form.

Seema Khanna

Abstract

Due to the increase in the adoption of productivity and collaboration tools, along with the pressure to make mobile and other smart computing devices "network ready", the workload on IT industry is monotonically increasing. Data centre that house the systems necessary to support the organization have grown rapidly in scale and complexity. Much of this growth has occurred in an ad hoc fashion, with many new systems added as and when required, such as including end point security controls to address challenges when they occur. This introduces multiple inefficiencies, including low levels of resource utilization, and makes re-envisioning security within the data centre infrastructure a challenging, yet necessary, task. With more companies focusing on their information systems (IS) and networks, a number of problems have emerged, the most significant of which is the issue of information security (Kuegah, 2006). Information technology is growing at a rapid pace. Data assimilation in the world of cyber space is increasing exponentially and the current socio-economic structure of society will always generate large amounts of raw data. IT services of the data centres are using advance technology to fulfill the organization's goals of securing this large volume of data. As a consequence the expertise of the infiltrators and the tools being used by them continue to grow. The net result is non-stop episodes of malicious attacks, destruction of data or information assets, and data theft among others.

In todays connected world, there is an increasing dependence on information and information assets. It has made it nearly impossible to run data without proper and smooth operation of its information systems and the associated security as data centre are primary targets for cyber-attacks. Hacking and threats to the information systems have increased significantly over the past decade. The exponential rise in attacks in a world of ever-evolving threats that can cause potentially catastrophic damage and may even one day lead to an organizational cyber fatality. What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries and the skillset to match. The purpose of the study is to provide effective security to the data centre according to the changing technology. This research thesis attempts to suggest a framework for security of data centres.

The research methodology used in this thesis adopts mix method approach; i.e. combining qualitative and quantitative routes of research methodology. And then, triangulation was used

to synthesize the findings from both qualitative (semi-structured interviews) and quantitative (questionnaire based survey). Different methodologies have been discussed as part of this research, with an attempt to arrive at possible security framework that can provide the required security with the current technological options available. In the exploratory phase of the research, key factors/variables identified from literature review were confirmed through focused group discussions. Along with this, views of experts from industry and academia were solicited on the subject matter as part of an informal process to gather information. The key components were identified and linkages among them were then validated through empirical research. A total of 177 items were identified which were classified under five heads namely, Physical Security, Information security, Operation Security, Network & Component Security and Skillset. Data collected through questionnaires regarding information security framework has been analyzed using Exploratory and Confirmatory Factor analysis. Various parameters that come out of the collected data were evaluated in terms of their factor loading. Factors having higher factor loading and hence higher impact have been taken into consideration and other factors have been clubbed into an associated class of factors or discarded. Structural Equation Modeling (SEM) has been used to model the factors and their linkages into a model, the model is formulated in AMOS, with inputs from structural equation models. An information security framework has thus been suggested in this study using SEM. The framework concludes that a secure network is dependent on skill set and network & component security. It is also concluded that one cannot deploy perfect security but one can approach to achieve the perfect security. The main aim of the security professionals should be few things like how fast the threat can be detected, what steps should be taken to stop the threat so that loss can be minimized, and how fast loss can be recovered so that availability should be maintained.

This study shall remain relevant for a certain period, the shelf life of which cannot be defined. However, a framework that relies on the expertise of the human resources in a data centre to deploy and implement it and with the constant advancement in this ever evolving field, this research shall remain a constant work in progress.

सार

उत्पादकता और सहयोग के उपकरण को अपनाने में वृद्धि के कारण, मोबाइल और अन्य स्मार्ट कंप्यूटिंग उपकरणों "नेटवर्क तैयार" बनाने के दबाव के साथ-साथ, आईटी उद्योग पर काम का बोझ एक समय में बढ़ रहा है। डेटा सेंटर जो संगठन की सहायता के लिए जरूरी प्रणालियों को घर में बड़े पैमाने पर और जटिलता में तेजी से बढ़ा है। इस विकास की अधिकांशता तदर्थ फैशन में हुई है, साथ ही कई नई प्रणालियां जोड़ दी गई हैं और जब आवश्यकता पड़ती है, जैसे अंत बिंदु सुरक्षा नियंत्रणों को चुनौतियों का सामना करने के लिए जब वे होते हैं यह कई अनावश्यकताओं का परिचय देता है, जिसमें संसाधनों के उपयोग के निम्न स्तर शामिल हैं, और डेटा सेंटर के बुनियादी ढांचे के भीतर सुरक्षा को पुनः प्रोजेक्ट करना एक चुनौतीपूर्ण, फिर भी आवश्यक कार्य है। अपनी सूचना प्रणाली (आईएस) और नेटवर्क पर ध्यान केंद्रित करने वाली अधिक कंपनियों के साथ, कई समस्याएं उभर गई हैं, जिनमें से सबसे महत्वपूर्ण सूचना सुरक्षा (क्यूगाह, 2006) का मुद्दा है सूचना प्रौद्योगिकी तेजी से बढ़ रही है। साइबर स्पेस की दुनिया में डेटा एकीकरण तेजी से बढ़ रहा है और समाज के वर्तमान सामाजिक-आर्थिक ढांचा हमेशा बड़ी मात्रा में कच्चे डेटा का उत्पादन करेगा। डेटा केंद्रों की आईटी सेवाओं, डेटा के इस बड़े मात्रा को हासिल करने के संगठन के लक्ष्यों को पूरा करने के लिए अग्रिम तकनीक का उपयोग कर रही हैं। परिणामस्वरूप घुसपैठियों की विशेषज्ञता और उनके द्वारा इस्तेमाल किए जा रहे उपकरणों का विकास बढ़ना जारी है। शुद्ध परिणाम दुर्भावनापूर्ण हमलों, डेटा या जानकारी की संपत्तियों का विनाश, और दूसरों के बीच डेटा चोरी के गैर-रोक एपिसोड है।

आज की दुनिया में जुड़ी हुई है, जानकारी और सूचना संपत्ति पर बढ़ती निर्भरता है। इसने अपने सूचना प्रणालियों के उचित और सुचारु संचालन के बिना डेटा को चलाने के लिए लगभग असंभव बना दिया है और संबंधित सुरक्षा साइबर हमलों के लिए प्राथमिक लक्ष्य हैं। पिछले एक दशक से सूचना प्रणाली में हैकिंग और खतरों में काफी वृद्धि हुई है कभी-विकसित खतरों की दुनिया में हमलों में घातीय वृद्धि जो संभावित रूप से विपत्तिपूर्ण क्षति हो सकती है और एक दिन भी एक संगठनात्मक साइबर मृत्यु के लिए आगे बढ़ सकती है। क्या आवश्यक है सूचना सुरक्षा का एक नया मॉडल, जो खतरों के ज्ञान से प्रेरित है, संपत्ति, और संभावित प्रतिद्वंद्वियों और कौशल को विकसित करने के उद्देश्यों और लक्ष्य। अध्ययन का उद्देश्य बदलते हुए प्रौद्योगिकी के अनुसार डेटा सेंटर को प्रभावी सुरक्षा प्रदान करना है। इस शोध थीसिस डेटा केंद्रों की सुरक्षा के लिए एक रूपरेखा का सुझाव देने का प्रयास करता है।

इस थीसिस में इस्तेमाल अनुसंधान पद्धति मिश्रण विधि दृष्टिकोण को गोद ले; अर्थात अनुसंधान पद्धति के गुणात्मक और मात्रात्मक मार्गों के संयोजन। और फिर, त्रिकोण का उपयोग किया गया था

गुणात्मक (अर्द्ध-संरचित साक्षात्कार) और मात्रात्मक (प्रश्नावली आधारित सर्वेक्षण) दोनों से निष्कर्षों को संश्लेषित करने के लिए इस शोध के एक हिस्से के रूप में विभिन्न तरीकों पर विचार-विमर्श किया गया है, जो संभव सुरक्षा ढांचे तक पहुंचने का प्रयास है जो मौजूदा तकनीकी विकल्पों के साथ आवश्यक सुरक्षा प्रदान कर सकता है। अनुसंधान के अन्वेषण चरण में, साहित्य की समीक्षा से पहचाने जाने वाले महत्वपूर्ण कारक / चर को ध्यान केंद्रित समूह चर्चाओं के माध्यम से पुष्ट किया गया। इसके साथ ही, सूचना इकट्ठा करने के लिए अनौपचारिक

प्रक्रिया के भाग के रूप में, उद्योग और शिक्षाविदों के विशेषज्ञों के विचार विषय विषय पर मांगे गए थे। मुख्य घटकों की पहचान की गई और उनके बीच संबंधों को अनुभवजन्य अनुसंधान के माध्यम से मान्य किया गया। कुल 177 वस्तुओं की पहचान की गई, जिन्हें पांच प्रमुखों, शारीरिक सुरक्षा, सूचना सुरक्षा, ऑपरेशन सिक्योरिटी, नेटवर्क और घटक सुरक्षा और कौशल के तहत वर्गीकृत किया गया था। सूचना सुरक्षा ढांचे के बारे में प्रश्नावली के माध्यम से एकत्र आंकड़ों का विश्लेषण किया गया है जो एक्सप्लोरेटरी और कन्फर्मैरिन्ट फैक्टर विश्लेषण का उपयोग किया गया है। एकत्रित आंकड़ों के बाहर आने वाले विभिन्न मानकों का मूल्यांकन उनके कारक लोडिंग के संदर्भ में किया गया था। उच्च कारक लोड होने वाले कारक और इसलिए उच्च प्रभाव को ध्यान में रखा गया है और अन्य कारकों को संबद्ध कारकों में जोड़ा गया है या हटा दिया गया है। स्ट्रक्चरल इक्विशन मॉडलिंग (एसईएम) को कारक मॉडल के रूप में इस्तेमाल किया गया है और एक मॉडल में उनका संबंध है, मॉडल को एमओएस में तैयार किया गया है, संरचनात्मक समीकरण मॉडल से इनपुट के साथ। इस प्रकार इस अध्ययन में एसईएम का उपयोग कर सूचना सुरक्षा ढांचा का सुझाव दिया गया है। फ्रेमवर्क निष्कर्ष निकाला है कि एक सुरक्षित नेटवर्क कौशल सेट और नेटवर्क और घटक सुरक्षा पर निर्भर है यह भी निष्कर्ष निकाला गया है कि कोई पूर्ण सुरक्षा तैनात नहीं कर सकता है, लेकिन एक पूर्ण सुरक्षा प्राप्त करने के लिए संपर्क कर सकता है। सुरक्षा पेशेवरों का मुख्य उद्देश्य कुछ चीजें होनी चाहिए जैसे खतरे को कितनी तेजी से पता लगाया जा सकता है, खतरे को रोकने के लिए कौन से कदम उठाए जाएं ताकि नुकसान कम किया जा सके, और कितनी तेजी से नुकसान ठीक किया जा सके ताकि उपलब्धता को बनाए रखा जा सके।

यह अध्ययन एक निश्चित अवधि के लिए प्रासंगिक रहेगा, जिसके शेल्फ जीवन को परिभाषित नहीं किया जा सकता है। हालांकि, एक ढांचा जो एक डेटा केंद्र में मानव संसाधन की विशेषज्ञता पर निर्भर करता है, इसे लागू करने और उसे क्रियान्वित करने और इस विकसित विकसित क्षेत्र में निरंतर प्रगति के साथ, यह शोध प्रगति में एक निरंतर काम होगा।

Table of Contents

List of Figures

List of Tables