Evaluating the Wannacry Ransomeware and Developing a roadmap to prevent the potential Risk:
With Special reference to South Eastern University of Sri Lanka

Mohamed Musthafa Mohamed Arsath
Assistant Network Manager
South Eastern University of Sri Lanka

arshadmmm@seu.ac.lk

Mr.Lakamal Rupasinghe
Senior Lecturer
Sri Lanka Institute of Information Technology
lakmal.r@sliit.lk

Abstract: Information is one of the most prominent assets for Universities and must be protected from wannacry and other malware. This paper analysed the wannacry ransomware threat specifically evolve in University's network, and this research proposed information security framework for University network environment. The proposed framework reduces the risk of wannacry by supporting three phase activities; the first phase assesses vulnerabilities of assests in order to identify the weak point in computer networking assets, the second phase focuses on the risk level of individual assets and university level, the third phase of risk assessment model develops a roadmap to implement security controls in order to protect from wannacry and improve University's security position. The proposed framework is applied on South Eastern University of SriLanka. Computing environment and the evaluation result showed the proposed framework enhances the security level of University campus network. Risk assistant network manager and system analyst of University to perform reliable and repeatable risk analysis in realistic and affordable manner can use this model.

Keywords: Threat, University, vulnerability, WannaCry ransomware

I.INTRODUCTION

With developing Information and Communication Technology, computing environment and network become an important part in the world. New services are increasing the same time the technology develop and campus network become an important role to run academic program in the university. Campus network provides lots of ICT services to students, staff such as online registration, online assignment submission, digital library, LAB facilities connecting with servers, administrative task, WIFI and so on. All are using advanced computing resources and its developing day by day by implementing new services and students and staff using unlimited internet access for the academic and personal usage. Therefore, the sometime developing technology provides us security threats to university network which large and open. Cyber-attacks happen frequently everywhere because cyber criminals try to take advantages such as financial gain, competition between countries and companies and most of the people are doing this for a hobby. Therefore, Confidentiality of Information, integrity of information and availability of information are the risk parts in the cyber-attack. Therefore, everyone in the digital world pushes to ensure his or her security of

ICT resources. Ransomware is a malware that encrypts contents on infected systems and demands payment in bitcoins. WannaCry Ransomware is a type of malicious software that designed to block access to a windows computer system until a ransom is paid. more than 60 chinses universities were affected by WannaCry last year. **Therefore, protecting campus network become crucial**. This paper proposes Qualitative Information Security Risk Assessment Model designed specifically for campus network to identify the risk level of wannacry ransomware. The proposed model qualitatively measures the security risks by identifying vulnerabilities within Universities windows system configuration. This model can be used by Assistant Network Manager and system analyst or any security managers of University to perform reliable and repeatable risk analysis in realistic and affordable manner.

II.RELATED WORK

The Wannacry ransomware that spread across the globe last year and affected chines universities as well. According to Chinese cyber security giant Qihoo 360's Threat Intelligence Centre. Almost 30,000 organizations across the country were affected in all. Wannacry ransomware attacked more than 66 universities out of 1600 in china. Carnet said the 66 universities were affected mainly because their operating systems were not regularly upgraded rather than any major security shortcomings. It dismissed Qihoo 360's claims as "inaccurate statements that have seriously misled public opinion, caused panic among teachers and students, and affected the normal order of instruction and life".

Beijing University and Tsinghua University, China's two top institutions located in Beijing, issued statements saying prompt security action had prevented a "large-scale" infection on their campuses. They gave no further details.

Students in campuses affected by the ransomware, however, told of their horror finding their experiment data encrypted and half-completed theses files lost, which could affect their graduation, according to Chinese media reports

Computer Emergency Readiness Team | Co-ordination Center (CERT|CC) is an expert group that handles computer security incidents. They said WannaCry has been detected in Sri Lanka as well. CERT had received a complaint regarding a computer in an institution in Colombo, which had been infected with the ransomware virus. They said the infected computer had not been updated nor did it include an updated virus guard. However, the CERT team had managed to clean the virus from the computer and restore the system with an update and they said the virus had affected none of the other computers as the operating system had been updated. The institution had also taken the precaution of backing up its data as a security measure.WannaCry ransomware attacked several countries all over the world and there are no proper planning to prevent WannaCry threat since its being developed in other format continuously. The awareness is very less and there was no much research done in Sri Lanka. Generally, Campus network and students are not well aware about WannaCry and not adopted for best security practicesThere are various risk assessment models available, some of which are qualitative while others are quantitative in nature.. In order to improve security organization system some standard principles are needed. There are various risk assessment models available for analyzing risk, some of which are qualitative while others are quantitative in nature; having a common goal of estimating the overall risk value . OCTAVE, NIST RMF, ISO and so on.

There are numerous risk assessment models; however, there is no mechanism to assist organizations in determining which model is the best to be employed within an organization; also these models considered the security challenges identified in hacking target organizations like banks. Although security risk assessment is crucial for these organizations but these organizations have secure and close network environment. On the other hand, higher educational institutions like Universities where information security risk assessment is major and high priority job are having large and open computing environment. The next section describes the typical scenario of University network environment comprises of diverse small network.

III. SOUTH EASTERN UNIVERSITY NETWORK SETUP

Fig. 1 shows network setup of South Eastern University of Sri Lanka that comprises of diverse small networks and maintain several VLANs. With the rapid development of technology, universities strive to develop a convenient and valuable learning environment through IT technologies. University large computing environment includes diverse network devices, various software applications and many servers.

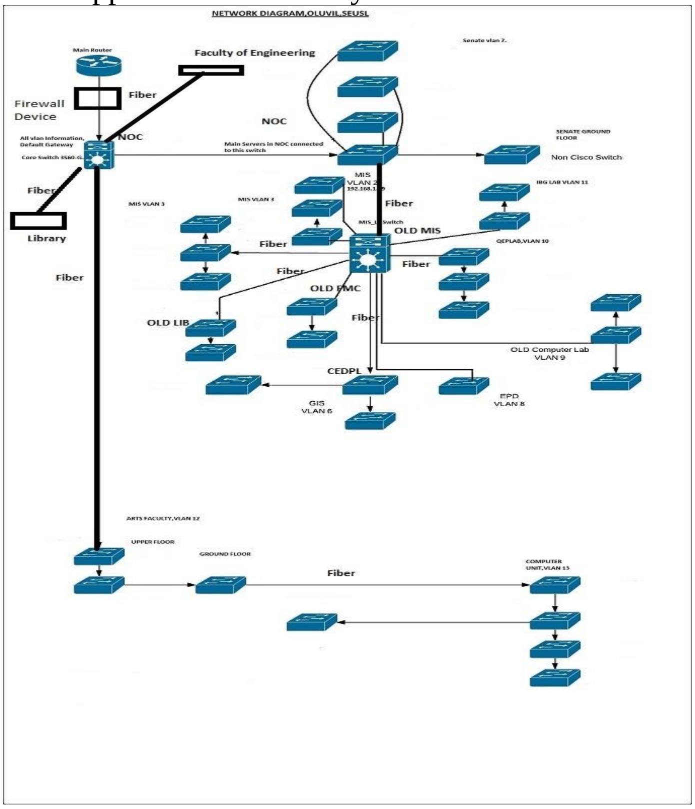
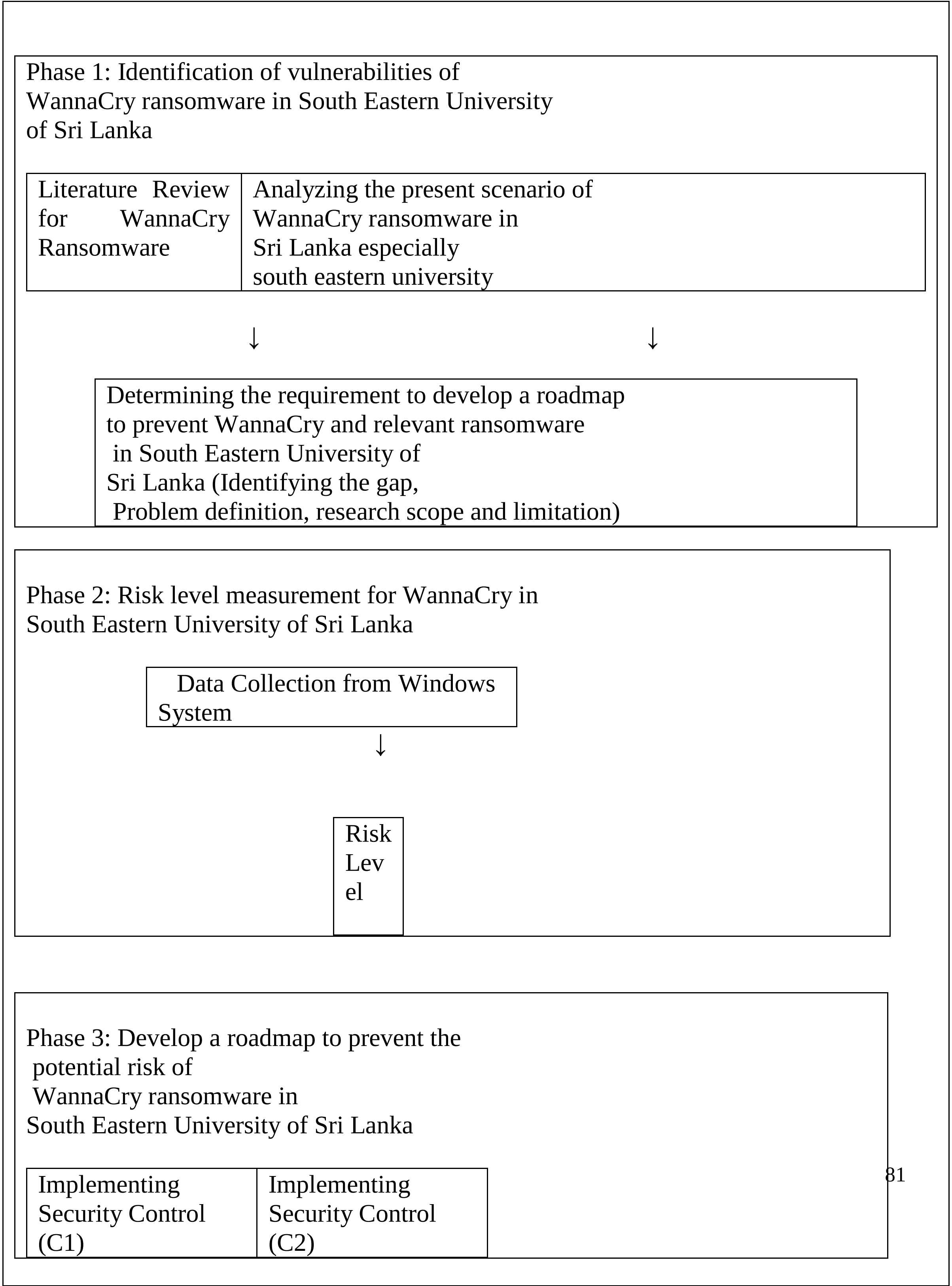


Figure 1 Network Diagram of South Eastern University of Sri Lanka

South Eastern University is a state university in Sri Lanka. There are around 4000 students and 600 staff working in South Eastern University. There are six faculties and several departments including Administrative section. Faculty of Engineering, Faculty of Applied science, Faculty of Technology, Faculty of Arts and Culture, Faculty of Islamic studies & Arabic language and Faculty Management & Commerce. South Eastern University provides ICT infrastructure for students and staff. There are different combinations of network devices such as firewall device, router, servers, network switches, Wireless Access Points and network computers with windows operation systems. As Internet service, cabling and Wi-Fi internet access are provided. Students' access local servers for the academic purpose and staff also access local servers for administrative purpose. Confidentiality, availability and Integrity of the assets must be ensured. There 1000 computers altogether that staff and students are using and several laptops and android devices are using Wi-Fi access. Windows machines are samples, which is vulnerable to WannaCry attack. We can identify the vulnerable port, protocol and OS of WannaCry in windows machine.

IV. PROPOSED QUALITATIVE INFORMATION SECURITY RISK ASSESSMENT MODEL

This research is comprised of three phases: identify the vulnerabilities of WannaCry in South Eastern University of Sri Lanka. Qualitative risk level measurement for WannaCry and Develop a roadmap to prevent the potential risk of WannaCry ransomware. **Error! Reference source not found.** Figure 2 Risk Methodology
illustrates the research methods that were used to meet the objectives in each phase:



Phase 1: Identification of vulnerabilities of WannaCry ransomware in South Eastern University of Sri Lanka
Literature Review for WannaCry Ransomware
Analyzing the present scenario of WannaCry ransomware in Sri Lanka especially south eastern university
Determining the requirement to develop a roadmap to prevent WannaCry and relevant ransomware in South Eastern University of Sri Lanka (Identifying the gap, Problem definition, research scope and limitation)
Phase 2: Risk level measurement for WannaCry in South Eastern University of Sri Lanka
Data Collection from Windows System
Risk Lev el
Phase 3: Develop a roadmap to prevent the potential risk of WannaCry ransomware in South Eastern University of Sri Lanka
Implementing Security Control (C1)
Implementing Security Control (C2)

Figure 2 Risk Methodology

Phase 1

This phase begins with assets related with WannaCry ransomware and find the vulnerabilities in the assets in South Eastern university of Sri Lanka. This will show the current security status and it is effective on WannaCry. Then we can analyze the effectiveness of security controls.

Phase 2

Data collection starts with vulnerability scanning of vulnerable Operating system, ports and protocols of WannaCry in computers of staff, students and servers of South Eastern university of Sri Lanka. After data collection, vulnerability and risk level will be identified in individual asset and entire university risk factor averagely.

Phase 3

This phase mainly focuses on implementing security controls. Then we can identify risk treatment and prioritize the security controls will be given to mitigate the risk of WannaCry. We can prioritize controls. Finally, a roadmap will be given to the South Eastern University of Sri Lanka to implement the recommendation

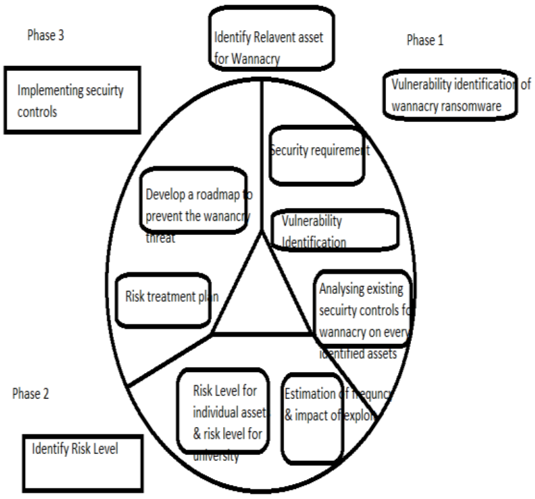

Phase 3
Identify Relavent asset for Wannacry
Phase 1
Implementing secuirty controls
Vulnerability identification of wannacry ransomware
Security requirement
Develop a roadmap to prevent the wanancry threat
Vulnerability Identification
Risk treatment plan
Analysing existing secuirty controls for wannacry on every identified assets
Phase 2
Risk Level for individual asset & risk level for university
Estimation of frequncy & impact of exploit
Identify Risk Level

Figure 3 The Proposed Risk framework

Error! Reference source not found.. The main objective behind designing a security risk assessment framework is, “security controls should be selected based on real risks of WannaCry to an organization’s assets and operations”. Numerous of security risks assessment models are available but University computing environment differ from other organizations as it is large, open and consists of several small diverse network with various users. Selecting risk assessment model without analysis, results in implementation of security controls in the wrong places, wasting of resources and leaving an organization vulnerable to unanticipated threats. The proposed risk assessment model initially analyses what is to be assessed, who needs to be involved and the criteria for quantifying, qualifying, and comparing severity of risks. The assessment results must be documented properly. The goal of proposed framework is to measure risk level qulititatively that will allow higher educational institutes to understand security risks. The proposed model is based on the most popular risk frameworks in use today, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), developed at Carnegie Mellon University. The proposed framework performs three phase activities to make standard model more absolute, and provides a practical approach, which can be used in real educational environment

A. Assets and stakeholders' identification

The risk assessment techniques require to clearly specifying the assets. This step of proposed model defines the boundaries and contents of the asset to be assessed. In proposed framework, information is taken as an asset.

B. Understanding security requirements

In this step, along with the resources and the information that constitute the system, the boundaries of the IT system will be identified. This step defines the scope of the risk assessment effort and provides information essential to defining the risk. The input for this step is information about hardware, software, data, port, protocol and information, network connections and system interfaces; and the output is a document that describes system mission, system boundary, system functions and information about criticality and sensitivity of data.

C. Threats and vulnerabilities identification

In this step, threat is WannaCry ransomware. We analyze the associate port, protocol and OS information.

D. Analysis of Effectiveness of Controls

In this step of assessment technical controls like vulnerable port, protocol, windows, OS and its updates are considered and a document is prepared as an output, which describes the effectiveness of system in defending against the particular threats.

E. Qualitative Risk Measurement

Identified individual asset's risk factor can be measured by running a script and the average risk level can be measured by calculating the vulnerable machines in every faculties and departments as per the sample size. The qualitative risk level can be determined in the range low to high. This risk level will be further used in creation of remediation plans.

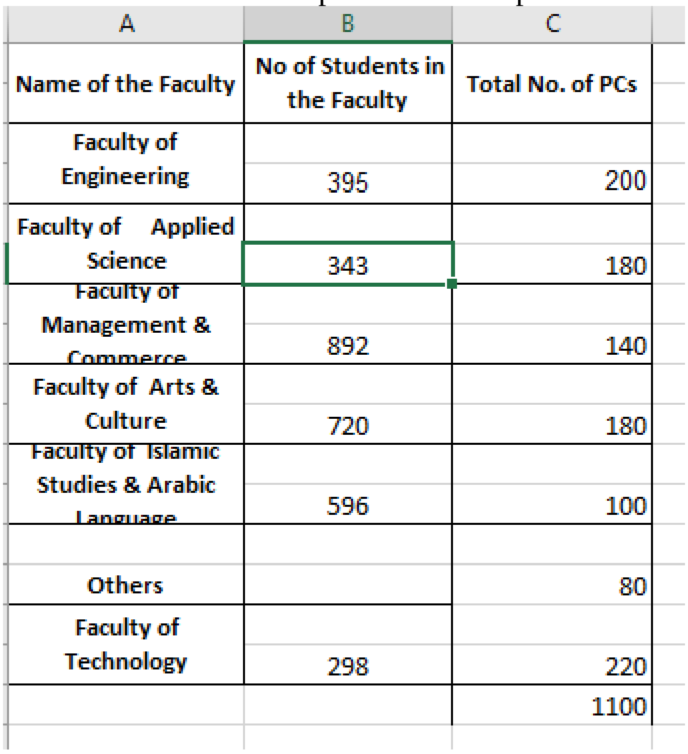
F.Creation of Actionable Remediation Plan

Risk level found in previous step show the risk level, which assists in defining remediation plans to validate identified vulnerabilities in order to improve system's security level. Second phase of the proposed identifies the areas are having the individual risks of associated vulnerable assets of WannaCry and entire university's risk level using can be calculated by finding the average value of the vulnerable machines. The remediation plans will be designed using this information.

G.Drive Decisions Using Powerful Reporting

After completion of risk assessment procedure, the results should be documented in an official report format. This report will help senior management, the mission owners in making decisions on policy, procedural, budget, and system operational and management changes. As risk assessment is recursive procedure, this final generated report will be used as an input of phase1 of proposed framework in the next cycle of risk assessment procedure.

Table 1 No of Computers and Sample Size

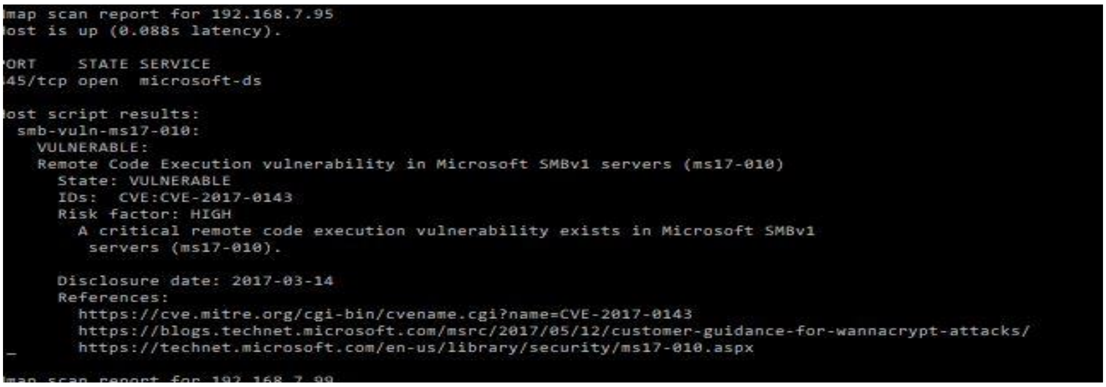


Name of the Faculty	No of Students in the Faculty	Total No. of PCs
Faculty of Engineering	395	200
Faculty of Applied Science	343	180
Faculty of Management & Commerce	892	140
Faculty of Arts & Culture	720	180
Faculty of Islamic Studies & Arabic Language	596	100
Others		80
Faculty of Technology	298	220
		1100

The sample size was selected in a way that to be conducted and also to be representative of the population. The researcher decided to conduct 280 windows computers. These are included Students LABs in several faculties and staff in all the faculties. The sample size is limited due to the cost, time constraints and population size. For the purposes of this research, port and protocol scanning NSE script was used to identify the vulnerabilities since it is the main data for our research

V. EVALUATION OF PROPOSED INFORMATION SECURITY RISK ASSESSMENT MODEL

University network is continuously expanded and modified, its components changed, and its software applications replaced or updated with newer versions; these changes indicate that new risks will emerge and the previously mitigated risks may again become an issue, the risk management is ongoing and evolving process. This section emphasizes the good practice and need for an ongoing risk evaluation and assessment in order to improve security level. In order to evaluate the importance and effectiveness of proposed model, it is applied on South Eastern University of Sri Lanka Environment



```
map scan report for 192.168.7.95
ost is up (0.088s latency).

ORT     STATE SERVICE
45/tcp open  microsoft-ds

ost script results:
 smb-vuln-ms17-010:
   VULNERABLE:
   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
     State: VULNERABLE
     IDs:  CVE:CVE-2017-0143
     Risk factor: HIGH
       A critical remote code execution vulnerability exists in Microsoft SMBv1
        servers (ms17-010).

     Disclosure date: 2017-03-14
     References:
       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

map scan report for 192.168.7.99
```

Figure 4 Scan Result of a VLAN in South Eastern University of Sri Lanka

A.Implemented NSE script for port and Protocol scanning

```
nmap -Pn -p445 –script smb-vuln-ms17-010 192.168.0.0/24 –oN output.txt
nmap -Pn -p445 –script smb-vuln-ms17-010 10.194.0.0/17 –oN output.txt
```

Table 2 scan results of vulnerable computers of WannaCry

Faculty/Department	Samples Windows OS	Port 445 (open)	SMBV1 vulnerable
Faculty of Engineering	46	40	31
Faculty of Technology	31	04	2
Faculty of Management & Commerce	42	11	8
Faculty of Islamic Studies & Arabic Language	43	30	23
Faculty of Arts & Culture	40	15	11
Faculty of Applied Science	45	20	16
Admin & Others	34	28	25
Total	**280**	**153**	**118**

B. Qualitative Risk Level Measurement

Information security Risk assessment is the process of identifying vulnerabilities, threats and risks associated with organizational assets. Qualitative information security risk assessments are usually well received because they because they involve many people at different level of the organization. In addition, the controls that can mitigate these threats. This research was threat based risk assessment. WannaCry ransomware is the threat and unpatched MS 17-010 is a critical risk in Windows system.Port 445 is opened in 153 windows computers out of 280 computers and transport protocol SMBv1 is opened in 118 windows computers out of 280 computersTherefore, 118 windows computers out of 280 are critical since Microsoft defines this update as **critical.**

Percentage of risk magnitude level = 118/280 x 100

Percentage of the university Risk magnitude = 42%
Therefore, 42% of windows systems are in critical position and vulnerable to wannacry ransomware in South Eastern University of Sri Lanka

VI. RESULTS

This chapter presents the results of this study with the goal of preventing Wannacry ransomware and enhance security with awareness. As indicated in previous chapters, the primary purpose of this qualitative research study was to propose a roadmap to prevent the potential risk of Wannacry by implementing security control based on finding in South Eastern University of Sri Lanka Based on the findings from the risk assessment; the next phase of the proposed framework is to identify countermeasure upgrades that will reduce the risk levels. The previous phase of risk assessment identifies the port 445 with SMBv1 opened protocol is vulnerable for the WannaCry attack. **According to the analyses, risk of WannaCry in South Eastern University is medium category**

VII. UPGRADE RECOMMENDATION

Based on the finding from the risk assessment of WannaCry threats, next phase is to implement countermeasure. By implementing security controls ,South Eastern University can prevent the potential threat of WannaCry. In the previous phase identified the vulnerabilities of WannaCry threat in South Eastern University of Sri Lanka. This section presents the recommendation about identified risk of WannaCry.

A.Measures to prevent WannaCry/WannaCrypt Ransomware

Users and administrators are advised to take the following preventive measures to protect their computer networks from ransomware infection / attacks:

- Immediately patch identified Domain , DNS and DHCP server with Microsoft Security Bulletin MS17-010
- In order to prevent infection users and organizations are advised to apply patches to Windows systems as mentioned in Microsoft Security Bulletin MS17-010. Identified 118 vulnerable windows system must be patched immediately and all the windows server and windows clients must be scanned and patch immediately

• Microsoft Patch for Unsupported Versions such as Windows XP,Vista,Server 2003, Server 2008 etc.
• To prevent data loss Users & Organizations are advised to take backup of Critical Data
• Block SMB ports on Enterprise Edge/perimeter network devices [UDP 137, 138 and TCP 139, 445] or Disable SMBv1.

B.Network Segmentation

• Restrict TCP port 445 traffic to where it is needed using router ACLs
• Use private VLANs if your edge switches support this feature
• Use host based firewalls to limit communication on TCP 445, especially between workstations

C.for Users

• Deploy antivirus protection

- Block spam
- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.

- Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail.

D.for Campus Network

- Establish a Sender Policy Framework (SPF),Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) for your domain, which is an email validation system designed to prevent spam by detecting email spoofing by which most of the ransomware samples successfully reaches the corporate email boxes.

- Deploy Application whitelisting/Strict implementation of Software Restriction Policies (SRP) to block binaries running from %APPDATA%, %PROGRAMDATA% and %TEMP% paths. Ransomware sample drops and executes generally from these locations. Enforce application whitelisting on all endpoint workstations.

- Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.

E.If the system is infected by WannaCry / WannaCrypt Ransomware

- Immediately isolate the system from network
- Run cleanup tools mentioned on our website to disinfect the same
- Preserve the data even if it is encrypted
- Report incident to CERT-LK and local law enforcement agency

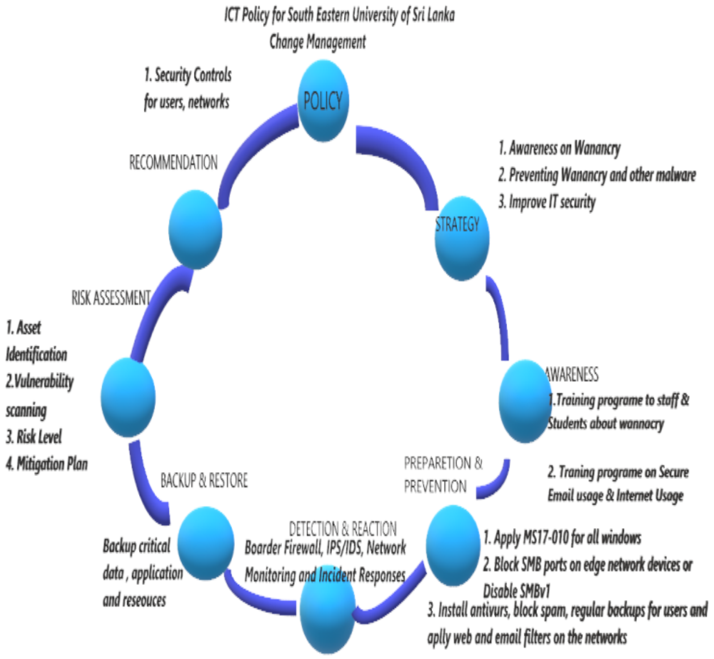

ICT Policy for South Eastern University of Sri Lanka
Change Management
1. Security Controls
for users, networks
POLICY
RECOMMENDATION
1. Awareness on Wanancry
2. Preventing Wanancry and other malware
3. Improve IT security
STRATEGY
RISK ASSESSMENT
1. Asset
Identification
2.Vulnerability
scanning
3. Risk Level
4. Mitigation Plan
AWARENESS
1.Training programe to staff &
Students about wannacry
BACKUP & RESTORE
PREPARETION &
PREVENTION
2. Traning programe on Secure
Email usage & Internet Usage
DETECTION & REACTION
Boarder Firewall, IPS/IDS, Network
Monitoring and Incident Responses
Backup critical
data , application
and reseouces
1. Apply MS17-010 for all windows
2. Block SMB ports on edge network devices or
Disable SMBv1
3. Install antivurs, block spam, regular backups for users and
aplly web and email filters on the networks

Figure 5 roadmap to prevent the potential risk of wanancry in South Eastern Univerity of Sri Lanka n

VIII. CONCLUSION

WannaCry ransomware is young academic field and need more researches on it. This research has presented a technological solution for the WannaCry ransomware prevention. Analysis existing vulnerabilities, effectiveness of existing security controls and risk assessment based on the vulnerabilities and recommending the security controls to prevent the WannaCry related ransomware and enhance the security of South Eastern University of Sri Lanka. This would help to make new security policies for South Eastern University for ICT Usage. The future research should be based on bringing this all procedure to software-based implementation to identify the vulnerabilities, analysis the effectiveness and finding the risk and making security updates automatically. All type of ransomware should be analysed via software implementation

ACKNOWLEDGMENT

The authors are highly thankful to South Eastern University of Sri Lanka for providing financial grant and support for this research project.

REFERENCES

[1]C. Joshi and U. Singh, "Information security risks management framework – A step towards mitigating security risks in university network", *Journal of Information Security and Applications*, vol. 35, pp. 128-137, 2017.

[2]2018. [Online]. Available: https://www.us-cert.gov/security-publications/Ransomware 2016. [Accessed: 14- Feb- 2018].

[3]C. Thorbecke, "Simple things you can do to protect against ransomware attacks", *ABC News*, 2018. [Online]. Available: http://abcnews.go.com/US/simple-things-protect-ransomware-attacks/story?id=47410339. [Accessed: 02- Mar- 2018].

[4]"The WannaCry ransomware attack", *Strategic Comments*, vol. 23, no. 4, p. vii-ix, 2017.

[5]"The WannaCry ransomware attack", *Strategic Comments*, vol. 23, no. 4, p. vii-ix, 2017.

[6]"wannacry 2017 attack affected - Google Search", *Google.lk*, 2018. [Online]. Available: https://www.google.lk/search?q=wannacry+2017+attack+affected&source=lnms&tbm=isch&sa=X&ved=0ahUKEwja87eAy4jXAhUC5CYKHWL4B4oQ_AUICigB&biw=136

6&bih=662#imgdii=IhkIZq7sHnib6M:&imgrc=Nt7qgc8gP_YtiM. [Accessed: 14- Nov-2018].

[7]2018. [Online]. Available: http://webcache.googleusercontent.com/search?q=cache:-LbG2_X_8eMJ:ijarcs.info/index.php/Ijarcs/article/download/4021/3642+&cd=1&hl=en&ct=clnk&gl=lk. [Accessed: 14- Mar- 2018].

[8]"5 Methods For Detecting Ransomware Activity", *NetFort*, 2018. [Online]. Available: https://www.netfort.com/blog/methods-for-detecting-ransomware-activity. [Accessed: 14- Nov- 2018].

[9]"Ransomware Preventive Methodology | Symantec Connect", *Symantec.com*, 2018. [Online]. Available: https://www.symantec.com/connect/articles/ransomware-preventive-methodology. [Accessed: 03- Jun- 2018].

[10]*Symantec.com*, 2018. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf. [Accessed: 06- Apr- 2018].

[11]"WannaCry detected in Sri Lanka: CERT|CC", *Dailymirror.lk*, 2018. [Online]. Available: http://www.dailymirror.lk/article/WannaCry-detected-in-Sri-Lanka-CERT-CC-129079.html. [Accessed: 14- Nov- 2018].

[12]"WannaCry Ransomware attack: SL on list of affected countries - Sri Lanka Latest News", *Sri Lanka News - Newsfirst | Breaking News and Latest News provider | Political | Sports | International | Business*, 2018. [Online]. Available: https://www.newsfirst.lk/2017/05/wannacry-ransomware-attack-sl-list-affected-countries. [Accessed: 09- Feb- 2018].

[13]"Ransomware – what is it and how to remove it | Anti-ransomware", *Avast.com*, 2018. [Online]. Available: https://www.avast.com/c-ransomware. [Accessed: 16- Aug- 2018].

[14]M. Sekhose, "WannaCry ransomware attack: Microsoft Windows 7 most affected OS, XP count insignificant says Kaspersky", *BGR India*, 2018. [Online]. Available: https://www.bgr.in/news/wannacry-ransomware-attack-microsoft-windows-7-most-affected-os-xp-count-insignificant-says-kaspersky/. [Accessed: 07- Sep- 2018].

[15]"How to Detect SMBv1 Use on Your Network Using Traffic Analysis", *NetFort*, 2018. [Online]. Available: https://www.netfort.com/blog/detect-smbv1-use-network/. [Accessed: 02- Feb- 2018].

[16]"Customer Guidance for WannaCrypt attacks", *MSRC*, 2018. [Online]. Available: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer- guidance-for-wannacrypt-attacks/. [Accessed: 09- Jul- 2018].

[17]"MSRC - Microsoft Security Response Center", *Technet.microsoft.com*, 2018. [Online]. Available: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx. [Accessed: 04- Jun- 2018].

[18]"CVE -CVE-2017-0143", *Cve.mitre.org*, 2018. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143. [Accessed: 03- May-2018].

[19]"cldrn/nmap-nse-scripts", *GitHub*, 2018. [Online]. Available: https://github.com/cldrn/nmap-nse-scripts/wiki/Notes-about-smb-vuln-ms17-010. [Accessed: 14- Apr- 2018].

[20]M. Ghazouani, S. Faris, H. Medromi and A. Sayouti, "Information Security Risk Assessment A Practical Approach with a Mathematical Formulation of Risk", *International Journal of Computer Applications*, vol. 103, no. 8, pp. 36-42, 2014.

[21]"Analyzing Ransomware and Potential Mitigation Strategies", 2018. .

[22]*An Overview of Threat and Risk Assessment*, 2018. .

[23]C. PASCARIU, I. BARBU and I. BACIVAROV, "Investigative Analysis and Technical Overview of Ransomware Based Attacks. Case Study: WannaCry", *International Journal of Information Security and Cybercrime*, vol. 6, no. 1, pp. 57-62, 2017.

[24]"Why China’s universities are so vulnerable to WannaCry virus attack", *South China Morning Post*, 2018. [Online]. Available: https://www.scmp.com/news/china/policies-politics/article/2094514/why-chinas-universities-are-so-vulnerable-wannacry. [Accessed: 03- Apr- 2018].

[25]"Lessons from WannaCry: How to avoid the next ransomware epidemic | TechBeacon", *TechBeacon*, 2018. [Online]. Available: https://techbeacon.com/lessons-wannacry-how-avoid-next-ransomware-epidemic. [Accessed: 02- Sep- 2018].

[26]"Ransomware: Best Practices for Prevention and Response", *Insights.sei.cmu.edu*, 2018. [Online]. Available: https://insights.sei.cmu.edu/sei_blog/2017/05/ransomware-best-practices-for-prevention-and-response.html. [Accessed: 02- Mar- 2018].

[27]"5 ways to protect from WannaCry ransomware hackers", *Mail Online*, 2018. [Online]. Available: https://www.dailymail.co.uk/sciencetech/article-4505300/5-ways-smaller-target-ransomware-hackers.html. [Accessed: 01- Nov- 2018].

[28]"Preventing the still present threat of WannaCry", *Pulseway.com*, 2018. [Online]. Available: https://www.pulseway.com/blog/preventing-the-still-present-threat-of-wannacry. [Accessed: 14- Mar- 2018].

[29]*Cyberswachhtakendra.gov.in*, 2018. [Online]. Available: https://www.cyberswachhtakendra.gov.in/documents/WannacryWannaCryptRansomware_CRITICAL_ALERT_CERT-In.pdf. [Accessed: 13- Mar- 2018].

[30]*Web.mit.edu*, 2018. [Online]. Available: http://web.mit.edu/itgc/docs/ITGC%20Security%20Roadmap.pdf. [Accessed: 03- Aug-2018].

[31]"Cyber Swachhta Kendra: Wannacry/ WannaCrypt Ransomware - CRITICAL ALERT", *Cyberswachhtakendra.gov.in*, 2018. [Online]. Available: https://www.cyberswachhtakendra.gov.in/alerts/wannacry_ransomware.html. [Accessed: 15- Sep- 2018].

[32]"Cyber Swachhta Kendra: Prevention of Ransomware Infections", *Cyberswachhtakendra.gov.in*, 2018. [Online]. Available: http://www.cyberswachhtakendra.gov.in/alerts/ransomware.html. [Accessed: 01- Feb-2018].

[33]M. Ghazouani, S. Faris, H. Medromi and A. Sayouti, "Information Security Risk Assessment A Practical Approach with a Mathematical Formulation of Risk", *International Journal of Computer Applications*, vol. 103, no. 8, pp. 36-42, 2014.

[34]X. YANG, "Analysis of risk evaluation techniques on information system security", *Journal of Computer Applications*, vol. 28, no. 8, pp. 1920-1923, 2008.

First Author https://www.researchgate.net/profile/Musthaffa_Arsath

Second Author https://www.sliit.lk/computing-faculty/staff/lakmal.r/