Mental Attitude of Ransomware among BYOD users: Awareness Framework

H.A.H.V. Halwatura[1#] and R.P.S Kathriarachchi[1]

[1]*Faculty of Computing, General Sir John Kotelawala Defence University, Ratmalana, Sri Lanka*
[#]*Corresponding author; <vee.viha@gmail.com>*

Abstract— *Ransomware has increased its degree of corruption by striking to Bring Your Own Devices(BYOD) in the interest of acquiring money by security unconscious users over the past few months. Supposing the user does not pay up the ransom, the cyber criminals will aim in taking down a whole network via its link between BYOD devices. This paper examines the level of awareness and comprehension of BYOD users on Ransomware and investigates the established degree of security they have used to safeguard their devices. The methodology used to conduct this research was an online survey distributed through Email, Social Media and a Video sharing website. The survey was successfully completed by 150 persons securing their anonymity. The empirical results suggest that majority of respondents are unaware about the term Ransomware and those respondents who are, have no clear understanding on how it works. Therefore, in conclusion, Majority of people were previously infected by malware although they have had security software installed in their devices therefore, people must be literate to take additional security measures to protect their devices and data such as using antivirus and firewall software from "reputable companies", Installing mobile updates and being conscious on what you click on. Continuous awareness programs are considered to be an effective method to mitigate the risks by Ransomware.*

Keywords— Ransomware, BYOD, Network threats and awareness

I. INTRODUCTION

Throughout the previous years, there has been a large number of different cyber-attacks from cyber criminals and they tend to keep increasing with the emerging of new technologies and devices. Although Cybersecurity professionals develop new ways to mitigate the risks and handle the attacks of various malwares, every day, every hour cyber criminals tend to produce a new type of malware into the public networks. Therefore, the professionals have to be at least one step ahead of the cyber-criminals.

The Cybernetic Global Intelligence says that 2016 is shaping up to be the "Year of Ransomware" (Burton, 2016). Ransomware is a malware that locks out the users from their data or devices and in order to unlock they have to pay a ransom. Sometimes paying this ransom will not unlock the data of the users but it will be a trick to make them pay. Ransomware is not targeted towards an individual, the device will get infected through a site or a download, therefore it can infect any random persons' device. However, a study by Christiaan Beek and Andrew Furtak (Christiaan Beek et al,2016) proposed an advanced type of Ransomware which is designed to target individuals. This malware not only infects home PCs but is also able corrupts their handheld devices such as smart phone, laptops and PDAs. These types of devices are named under the trend of BYOD.

An infection of a single BYOD device of an employee of a particular organization who uses his device to access the organization network can corrupt the entire network of the company. In most cases, this action happens unknowingly causing severe damages to individuals and companies by resulting in major data losses.

Most researches on ransomware presents the structure of Ransomware and how it increases its degree of corruption. A recent survey released by Symantec suggests that the attacks of ransomware are more likely to have an impact on the Mobile phones and tablets that work under the Android OS platform (Savage, 2015). Why? Because Android a more open platform because any user can install Apps in the Play Store but the Apples app store is more secured allowing only certified people to release Apps into the store.

This research study aims to analyse information about the basic knowledge of some random BYOD users on Ransomware. Key questions asked from people were whether they are aware of Ransomware, if so what is it, what kind of BYOD devices do they use, have they ever been infected by a malware and whether they have any security software installed on their devices. The format of

this papers includes the Background, Methodology, then results based on the Method, next the discussion along with the design and finally the conclusion followed with the reference.

II. RELATED WORK AND FINDINGS

Although the introduction of a Ransomware first appeared in 1985 known as PC Cyborg by Joseph Popp, it was heavily increased since 2005. Today, the two most circulated types of Ransomware are the Locker Ransomware which is focused in locking your devices and the other is Crypto Ransomware which seals you out from your data (Geiyer, 2014). The past researches of Ransomware do not focus much on the awareness and perception of this Ransomware. A study by a researcher in Bitdefender suggests that 32% of users who are not yet affected by Ransomware thinks it is less likely that they will get affected (Arsene, 2016). The most affective propagation methods of Ransomware are depicted in a study by Trey Herr (Trey Herr, 2014). Another study shows that the strongest solution for the Ransomware mitigation is the education to this Malware (Luo, 2007). By controlling the I/O requests and protecting the Master file table can also help in reducing the risks (Kharraz, 2015). With all the negativity in Ransomware, there are also mechanisms that can be innovated in the future to detect this Malware (Kirda, 2015).

III. METHODOLOGY

The strategy used to collect information for this research was an Online Survey targeted to a larger number of people. Both qualitative and quantitative methods were used in favour of getting a variety answers. The survey questions were based on the information from previous researches. The distribution of the survey was conducted for five whole months (December 2015 to April 2016) and in order to get more genuine responses, it was conducted anonymously. Media of distribution of the survey was via email, Social Media Sites such as Facebook and LinkedIn and YouTube (through google form survey web link), this enabled in targeting a wider audience in different fields and age groups.

Along with the basic guidelines to fill the form were the questions regarding the research and the questions were made direct and simpler for the easiness of the respondent therefore they will answer all questions or is less likely to skip some questions. Demographic details such as age and gender of the people were not captures as they are not stated as a priority requirement for the analysis. Although, whether they are schooling, in university or is employed was questioned along with of their field of study or employment.

The survey was incorporated with ten questions that mainly questioned on the number of hours they spent on the internet, for what mainly purposes they use the internet for, what are the BYODs they use, how familiar they are with the term ransomware, whether they use and security software and their experience to a malware. This includes two open ended question with all others being close ended with radio buttons and check boxes.

III. RESULTS

All results obtained from the survey are been analyzed and presented in this section. The Figure 1 demonstrates the percentage of school, university and the employed respondents. The highest percentage is indicated by the University level being 56%, the next highest is shown by the School level which is 19% and the employment sector indicated by 24%. Least is the other category being 1%.

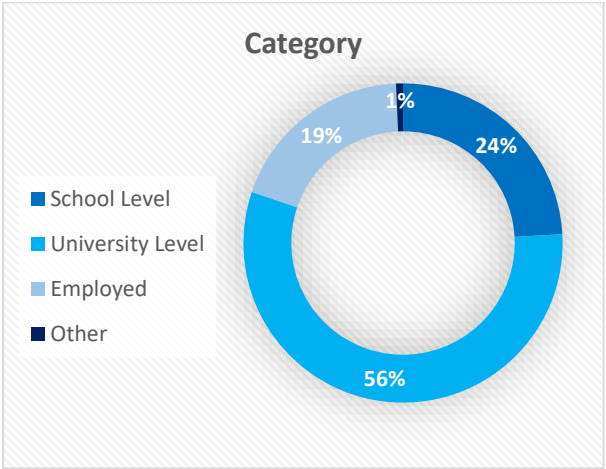
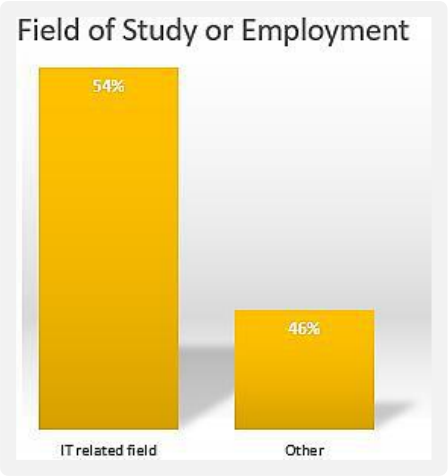


Figure 1. Category
Source: Author

Figure 2 surveys about the current field in which they are working or studying and as you can see below, the figure shows the percentage of other fields in contrast to the IT related fields. The IT related respondents were 54% whereas the other fields consisted of only 46%.



Respondents were then examined on how many hours they use a computing device and according to the results in

Figure 2. Field of study or employment
Source: Author

Figure 3, over 34% answered over 20 hours and 21% said for 1 to 5 hours and another 21% answered they use for 6-10 hours. 11-15 hours are used by a 11% where as a 7% answered 16-20 hours as their weekly usage of a Computing device. Only a 5% uses less than one hour.

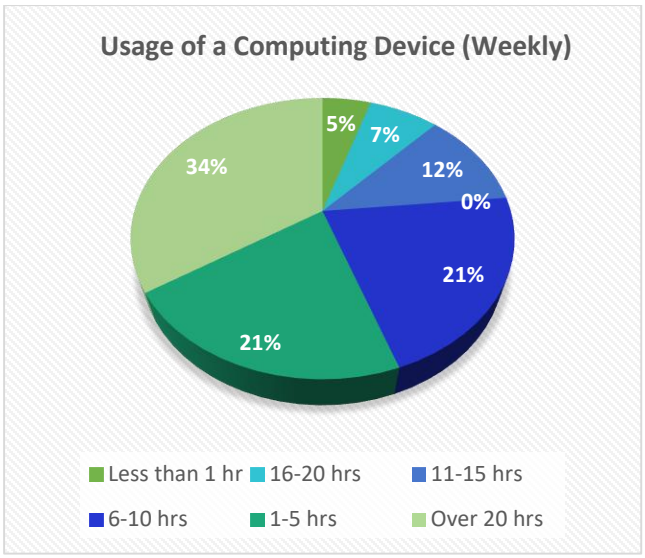


Figure 3 Usage of Computing Devices
Source: Author

The depiction presented below in Figure 4 is based on statistics of the mostly use BYODs. 74.10% uses Smart phones, Laptops are used by 65.60% whereas Tablets are only used by a 14.70%. All other devices that do not fall under these categories are represented in the other section consisting of only 2.80%.

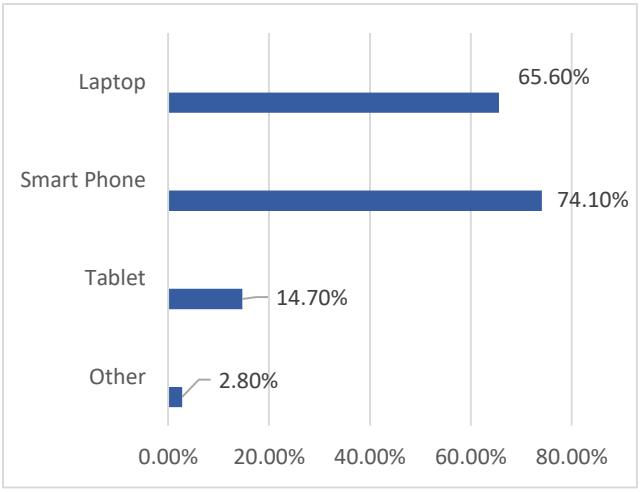


Figure 4 Heavily used BYODs
Source: Author

The next question as shown in Figure 5 was asked on the awareness of the term malware and a majority consisting of 72%(104 respondents) has not come through that term before, and only 28% (41 respondents) were familiar with it. The total number of respondents were 145.

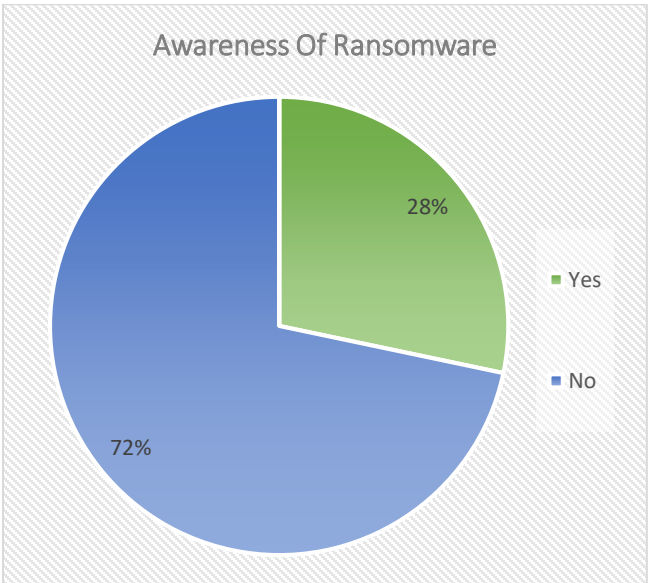


Figure 5 Ransomware Awareness

Source: Author

Table 1. Statistics of the Awareness of Ransomware

Source: Author

NO	IT related Fields	47%
	Other	53%
YES	IT related fields	50%
	Other	50%

Table 1 shows the results of the awareness of the term Ransomware in terms of the Figure 2 results that depicts the fields of the respondents. The results clearly show that the proportion of IT related fields to the other fields do not give a major difference.

From the respondents who answered 'Yes' in figure 5 were asked to choose the correct definition of Ransomware. Only a 57% chose the correct definition and the incorrect answers altogether were answered by the rest of the respondents. So from the respondents who has heard of the term Ransomware, around 43% do not know the correct definition it.

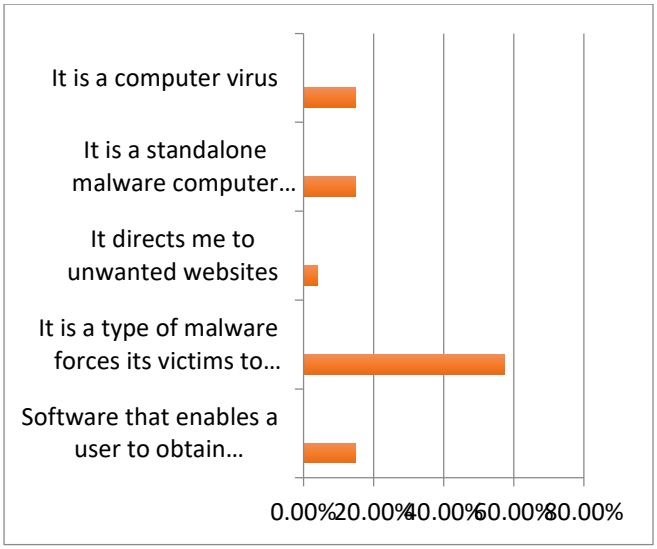


Figure 6. Selection of the most appropriate definition

Source: Author

The above Figure 6 was followed by an open ended question asked by the 41 respondents who are familiar with the term Ransomware allowing them to answer freely to collect their opinions and experiences. The question was based on 'How Ransomware work and how it can impact you?' The most common answers by the respondents are shown below in Table 2.

Table 2. The most common responses for the open ended

Source: Author

If you go to unwanted web sites you will get attacked by this	6%
Encrypts data and files and then prompts/ forces the user to pay to get a key to get back the data and files.	41%
Enters through a downloaded file and forces online payments by displaying false warnings about system being used for illegal activities.	6%
Phishing sites, fraud sites, Viruses, Malwares present in computer	4%
Dont know	43%

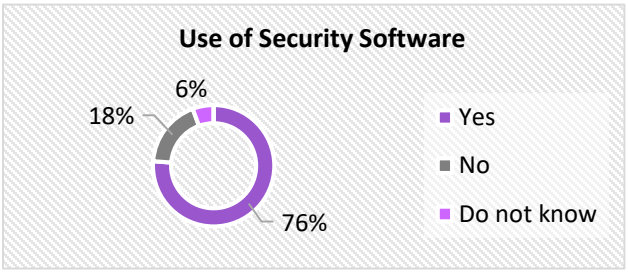


Figure 7. Usage of a Security Software

Source: Author

Figure 7 demonstrates that 76% of the respondents use a security software whereas only 18% do not use and 6% do not know whether they have a security software installed.

The next question as shown was based on their experience of an infection to any of their devices. As depicted in the Figure 8, although people who use a security software is 76%, they have been infected by a malware before. Only 25% has not yet being infected and 4% do not know whether they been or is infected.

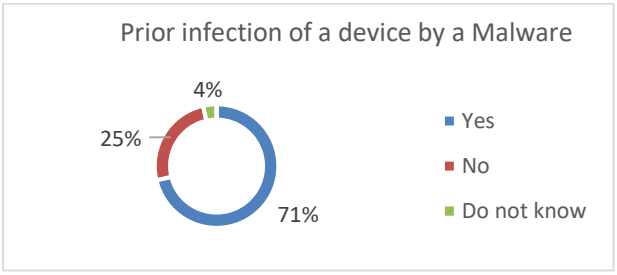


Figure 8. Percentage of Infected devices by a malware

Source: Author

The most used applications by the respondents via the Internet are shown by Figure 9. Education sites, Social Media sites, Music sites, Email, site for Sensitive storage of data and online shopping are the most popular categories of websites according to the respondents. An interesting indication of this question was the Email is used by 63.5% of the respondents and the download of Email attachments has been a major source of media for the distribution of Ransomware.

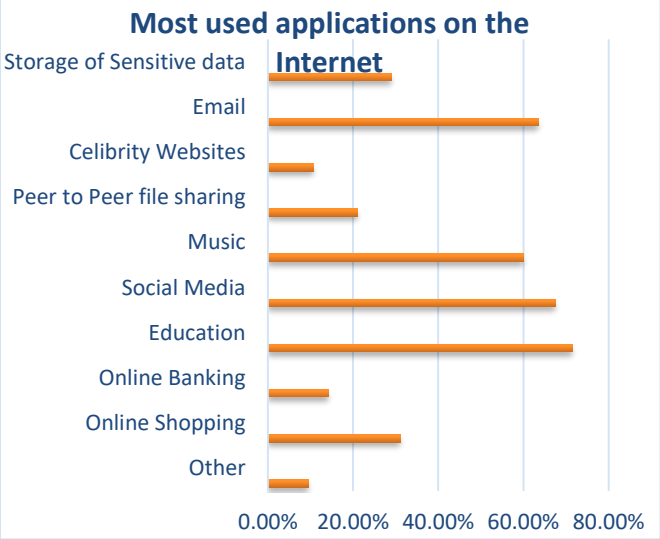


Figure 9. Most used applications on the Internet
Source: Author

IV. DISCUSSION

The results of this research has shown us that from a group of 150 people only a small proportion of people are fully aware of what is meant by a Ransomware and how it works. Although, some respondents are not literate about this Malware, they all use a BYOD which can directly corrupt their device as well the network they will connect to in an organization. The results indicate that majority of the respondents have faced a malware attack and only a very few does not use any security software and this does not mean that they will not have a chance of getting more malware attacks. This can mainly affect the people who are spending more than 20 hours on the Internet with their BYOD device depending on the most used applications. Even the results on the most used applications enabled us to see that the respondents are highly attached to the Entertainment Websites and Email which are strong medias in spreading malwares such as Ransomware and Spyware. However, the 76% of the respondents who use some kind of Software to protect their devices must keep their software up-to-date at all times.

Majority of the overall respondents of the survey are IT related people and via analysis it has been found that approximately 50% of the respondents who answered no to the question of whether they have come across the word Ransomware are in IT related fields. Another important question in the survey was the open-ended question which was helpful in getting the respondents experience and the understanding of the matter. This question was asked only from people who was familiar to the term Ransomware and not majority of the people could give clear explanation on how ransomware works or their effects. Although people are not fully aware about the Malware, they have an understanding that Ransomware is a threat. As mentioned before in this paper, the year 2016 has been categorize as the 'Year of Ransomware' so with the increase in awareness methods such as articles and news, people tend to get to know about the threats.

V. DESIGN

The framework in Figure 10 addresses many of the drawbacks in the literature. It illustrates a conceptual representation of factors affecting the research goals that direct the collection and analysis of data.

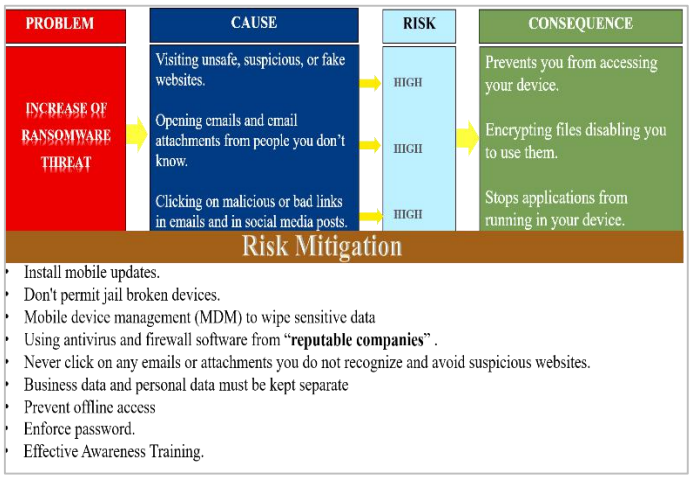


Figure 10 Awareness Framework
Source: Author

The key factors to consider are grouped into five areas:

- The main problem
- Cause
- Risk
- Consequences

- Solutions

These factors are interrelated to one another. First the main problem is being enumerated as the Increase of the threat Ransomware and then is the main causes such as visiting, opening or clicking of suspicious materials on the internet are being recorded along with their indication of risk as high. Next it shows the results due to your action and at last but most importantly it enumerates the solutions for preventing Ransomware.

VI. CONCLUSION

Ransomware is increasingly becoming an advanced threat that is aiming to target most of the users on the Internet and there can be many reasons how it can impact BYOD users and the networks they access to. According to the survey which was highly targeted on the younger generation, devices which are more likely to get infected are the Smart phones and Laptops. As the results depict, the majority of the respondents are unaware of this Malware and precautions must be taken to educate people on this subject especially the people who are dealing with the threat zone or who work with the applications which act as medium to spread Malwares, such as Email or insecure sites. Along with some recent incidents of Ransomware such as the infection of Apple Mac devices, people got to know about it up to a certain extent. Therefore, by articles and news people tend to get more aware about them. Considering all facts, priority must be assigned in educating people on Ransomware and relevant subjects. In conclusion, the main steps to be followed and executed by the BYOD users to mitigate the risks are Install mobile updates, Enforce password, Don't permit jailbroken devices, Business data and personal data must be kept separate, Mobile device management (MDM) to wipe sensitive data, Using antivirus and firewall software from "reputable companies", Prevent offline access, Never click on any emails or attachments you do not recognize and avoid suspicious websites, Effective Awareness Training, Avoid clicking on links or opening attachments or emails from people you don't know.

ACKNOWLEDGMENT

My deepest gratitude is extended to my Supervisor Mr. R.P.S. Kathriarachchi for the help and support he provided me in successfully completing this research paper.

REFERENCES

Alvarez M. (2015), What you need to know about ransomware, IBM.

Arsene L.& Gheorghe A. (2016), Ransomware. A Victim's Perspective, Bitdefender, viewed 24 February 2016.

Beek C. & Furtak A. (2016), Targeted Ransomware: No Longer a Future Threat, Intel Corporation.

Burton J. (2016), Don't Be Held Hostage: "Ransomware" On the Rise, Common Good Vermont, [online] Available at:https://blog.commongoodvt.org/2016/02/dont-be-held-hostage-ransomware-on-the-rise, [Accessed 10 March 2016].

Geiyer E. (2014), How to rescue your PC from Ransomware, PC World, [online], Available at:http://www.pcworld.com/article/2084002/how-to-rescue-your-pc-from-ransomware.html,[Accessed on 16 February 2016]

Herr T.(2014), PrEP: A Framework for Malware & Cyber Weapons, Cyber Security Policy and Reseach Institute, GW-CSPRI-2014-2.

Jaeger M.& ClarkeN.L.(2006), The Awareness and Perception of Spyware amongst Home PC Computer Users, SCISSEC & Edith Cowan University.

Kharraz A., Robertson W., Balzarotti D, et al(2015), CuttingtheGordianKnot:ALookUndertheHoodof Ransomware Attacks.

Kirda E. (2015), Most Ransomware Isn't As Complex As You Might Think Yes, we should be able to detect most of it, DIMVA 2015 in Milan, Italy.

Liao Q.(2007), Ransomware: a growing threat to smes, TX 78521

Liao Q.& Luo X. (2007), Awareness Education as the Key to Ransomware Prevention, 1065-898X print/1934-869X online.

Mercaldo F., Nardone C., Santone A.,et al (2016), Ransomware Steals your Phone. Formal Methods Rescue it, Department of Engineering, University of Sannio, Italy.

Savage K., Coogan P. & Lau H. (2015), The evolution of ransomware, Symantec Corporation.