Scientific Research Publishing

Int. J. Communications, Network and System Sciences, 2021, 14, 47-54
https://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

Improving the Cybersecurity Framework for Future Consumer Networks

Tyler Welker, Olatunde Abiona

Department of Computer Information Systems, Indiana University Northwest, Gary, USA
Email: tywelker@iu.edu, oabiona@iun.edu

How to cite this paper: Welker, T. and Abiona, O. (2021) Improving the Cybersecurity Framework for Future Consumer Networks. *Int. J. Communications, Network and System Sciences*, **14**, 47-54.
https://doi.org/10.4236/ijcns.2021.144004

Received: March 3, 2021
Accepted: April 27, 2021
Published: April 30, 2021

Abstract

The framework Information Technology professionals and Network Organizations use is often seen as open and dynamic. This can create many different pathways for cybercriminals to launch an attack on an enterprise network to cause panic, this situation could be prevented. Using the proposed framework, network administrators and networked organizations can improve their cybersecurity framework for future consumer networks. Implementing a network security plan that is up to date and outlines responsibilities of team members, creating a government subsidy to implement and increase safeguards on US based networks, and the analyzing of past cyber-attacks metadata to further understand the attacks that are causing problems for consumer networks can improve the cybersecurity framework for consumer networks and increase potential security on US based networks. Research found that the implementation of security plans, creating a government subsidy, and analyzing past metadata all show signs of improving the framework of cybersecurity in consumer based networks.

Keywords

Cybersecurity, Information Technology, Network Security, Malware, Attacks

1. Introduction

Information Technology (IT) and Network Organizations are described by words such as "open", "virtual", and "dynamic" [1]. This leads to cyber-attackers and hackers to constantly try to infiltrate networks through means of DDOS attacks, phishing attacks, social engineering attacks, and many other types of cyber-attacks. According to PurpleSec publication, Cyber security trends in 2021. Figure 1 shows the rates at which malware infection growth increased by millions over the years 2009-2018. In just nine years, the amount of malware infections increased by 800 million infections, from 12.4 million rising to 812.67 million.

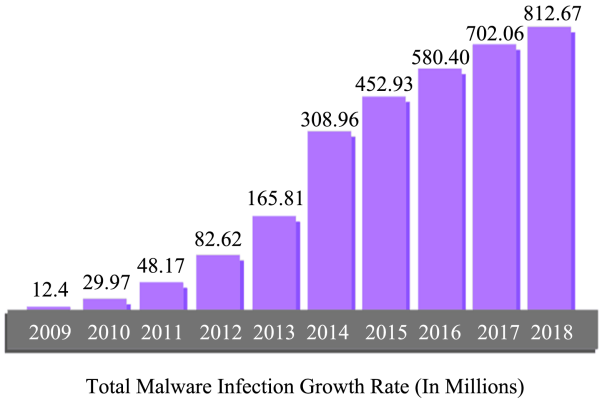

Figure 1. Total malware infection growth rate.

The increase of malware attacks is only one spectrum of cyber-attacks that are carried out on networks and systems around the world. Due to the dynamic and everchanging landscape of the IT field, unfortunately there is no set "guideline" for network administrators to follow each and every time, it is up to the Network Administrators to set up a proper preventative plan, and make the correct decisions to keep the network secure.

By creating a proper framework for Network Administrators to use to properly manage the networks risk management and risk assessment.

The increase of cyber-attacks on computers and networks across the world and the United States is increasing with each year, a proposed solution would be to create a government subsidy to implement and increase safeguards on US based networks. A major part of this proposed strategy would be using a team of government technicians to find these attackers and execute a counter-attack called a "hack-back".

This proposed hack-back is implemented to try and neutralize the attackers and make it difficult for them to have access to funds or means to continue to execute their attacks after they have to fix their systems from the US government's cyber-attacks. To achieve this private firm should be given the latitude to experience with active countermeasures, while still being under government subsidy to ensure no rules or regulations are being crossed [2].

With the increase of different types of cyber-attacks, the use of past metadata to understand the most likely chances of an attack and what type of attack that may be can help increase the chances a network can fight off an attack. Creating datasets of past metadata to understand the different types of attacks executed on systems in the past years, can help create an easier path to understand who is creating problems with the network and how to stop them efficiently.

This can be done by recording the different attacks on the network, but also all networks across an area or country, then reviewing that data and finding out the most popular means of attacks, and who carries those attacks out. Creating a preventative dataset can help decrease downtime in networks by already having a set solution in hand ready to go.

Using a proper framework to manage risks on a network, increasing government regulation on a hack-back team, and creating sets of metadata to review and understand possible upcoming attacks can all be used to improve the cybersecurity framework for future consumer networks. IT companies and Internet Service Providers try to eliminate down time as much as possible so their consumers are not without service for long periods of time, creating a plan to preventatively defend against attacks can cut downtime drastically moving forward.

The rest of the paper is arranged as follows: Section 2 highlights previous work done, In Section 3 we present our design methodology and finally the paper concludes in Section 4.

2. Literature Review

In network security, the primary way companies or network administrators can protect their network is by creating a network security plan that outlines all responsibilities of team members of the network administration team, as well as the preventative measures to ensure the safety of the network. The chances that a firm's information systems are not properly protected against certain kinds of damage or loss is known as "systems risk". The underlying problem with systems risk is that managers are generally unaware of the full range of actions that they can take to prevent risk [3]. The creation of a cyber security plan and protocol can help minimalize the systems risk of a company's software and hardware.

If the network administrators wait till the last possible minute to implement strategies to nullify the systems risk, it has been proven to be much less effective and the attacks are that much more devastating. **Figure 2** shows a framework of the relationship between risk management to risk assessment, adopted from OCTAVE. This figure shows that while creating a proper network security plan, network administrators can achieve this by continuously evaluating their risk management measures versus the risk assessment measures.

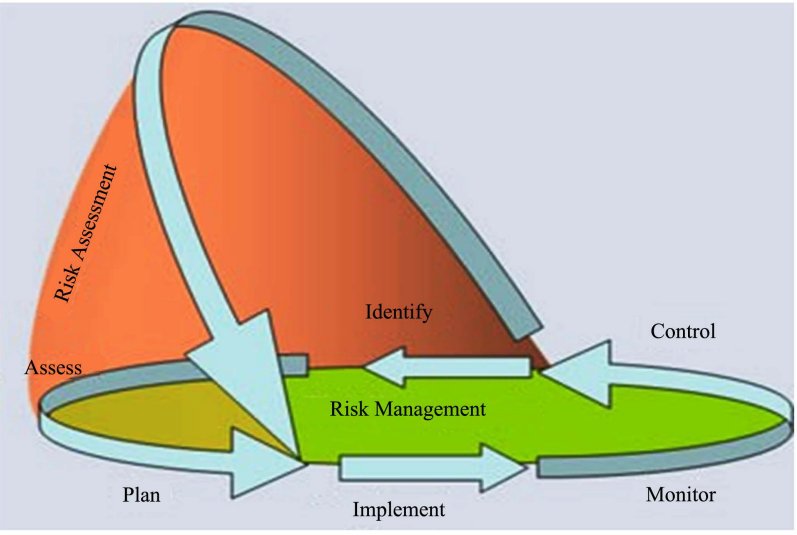

Figure 2. Relationship of risk management to risk assessment.

Risk management is a recurrent activity that deals with the analysis, planning, implementation, control and monitoring of implemented measurements and the enforced security policy. On the other hand, Risk Assessment is carried out at specific time points (ex. once a month, year, on demand, etc.) and until the performance of the next assessment provides a temporary view of assessed risks and while providing a feedback of parameters of the entire Risk Management process. The network administrator first off creates a plan, following the plan would be the implementation then monitoring of the plan that the network administrator has put in place. After monitoring then it would go to the control phase of the plan, at this point if there is a risk associated that the team has found; they can then identify, assess, and then plan again accordingly to the attacks that are taking place on the network. This loop creates a simple structure for teams to follow to ensure that their security plan is in constant adaptation to the many different attacks that can be presented.

The implementation of a plan can be accomplished in many different ways. One way that can accomplish the creation of a plan is to use The Taxonomic Framework of Security Methods and Connection to the Security Taxonomy written by Yejun Wu.

1) Identify the set of unique threats;

2) Determine the relevant risk factors that enhance the likelihood or vulnerability components of risk associated with each unique threat [type];

3) Establish the full set of controls to address each risk factor;

4) Specify the methods necessary to implement each control [4].

This control is a set of high-level mitigation measures. The first four steps of the security risk mitigation process can be illustrated as this:

Threat (implies)—Risk (mitigated by)—control (applied by) method [4].

The way that threats are then categorized creates a simple structure that shows a process and plan to stop the attacks on the network. Understanding the framework that Wu sets up by creating a series of guidelines to follow, and then can help develop a network security strategy. Identifying the set of unique threats shows the team what to expect from the problem itself. Determining the relevant risk factors that enhance the likelihood of vulnerability shows the team the items in the network infrastructure that are most vulnerable to these types of attacks. Establishing a full set of controls to each risk factor can create a solution to the problem at hand and can create options to solving the problem. Specifying the methods necessary to implement the control makes sure that the attack that the team just had to fight does not come back and re infect the network. Following this protocol can create clearer guidelines and solutions for the network team.

Along with creating a structure of a plan for network administrators to follow in the chance that there is an attack on the network. The creation of a team ran by the United States Government and The Department of Homeland Security, focusing on increasing the safeguards and controls on US based networks. Cyber-Terrorist groups primarily target the groups that can they can benefit from

the most, like political parties etc. On occasion, these groups stray away from focusing on big government groups that and change their focus to the civilian side. Creating a team of people to help the consumer side of the US networks can help deter the likelihood that an attacker would focus on the general population rather than a specific government entity.

While creating a government subsidy that primarily focuses on the security of consumer networks in the United States can help some problems, but there is also a responsibility from the consumer and the producers of the hardware and software to continuously improve security features to prevent possible future attacks against the population.

The primary focus of the government subsidy that would be created to help deter attacks against the general population would be to create a series of safeguards and controls throughout US based networks as well as the creation of a team to counter-attack possible incoming attacks. These types of counter attacks are called "hack-backs" and while there are some problems with the hack-back techniques, there are also ways that the government can use to their advantage.

This team of technicians that would be responsible for executing the counter-attacks would be also responsible for the general security and what is called "active defenses" for US based networks. In one documented case, a company re-routed a flood of incoming messages back to the sender-so an attack designed to temporarily shut down a website ended by shutting down the attacker's computer system [5].

While the possibility of hack-backs shutting down attacker's computer systems is possible, hardware and software can be replaced, and viruses and other malicious programs can be reloaded, where the humans controlling the systems are the most vulnerable. The team would then execute research on the attackers, finding out who they are, who their bosses are, and who is in charge of the whole operation. Once the team has identified the hackers, the suspects may be threatened with travel restrictions to Western Countries, restrictions on use of banks that move funds through Western banking systems, and other sanctions as well as companies that receive commercial secrets from data thieves might be threatened with sanctions in Western countries [5]. This is why the use of a government subsidy would make the most sense for implementing these rules and regulations against cyber-attackers, there would not be a way possible for a private sector to implement sanctions against major companies or firms, so the backing of a powerful government structure could help prevent further attacks.

3. Design Methodology

Creating this subsidy that conducts active countermeasures rather than having private companies conduct their countermeasures can create a clearer line of regulations and restrictions to what the team can or cannot do. The risks of hack-backs are real, and we should shape policy to minimize them, any such activity should be closely regulated by the government, we envision a three-part regulatory structure: the government should regulate who performs the hack-back,

supervise the targets for such action, and regulate the means [5].

The activity of hack-backs is still a very hard task to complete, and not every person is going to have the capabilities to do so, relying on a set of specialized contractors that are experts in their field. Another safeguard to ensure that the regulations are not taken out of hand, the government should keep a list of companies authorized to do such work, with membership card revoked for carelessness or recklessness. This task could be completed by the Justice Department, and could be done without any new legislation by listing the companies as "authorized" under the Computer Fraud and Abuse Act [5].

These regulations can be upheld by the contractors working with the government and deciding that a computer is likely beyond the reach of law enforcement, and such action is not contrary to US diplomatic goals [5]. Creating a series of checks and balances can ensure that the contractors are held responsible for their work and their actions, and also ensures that a contractor won't execute an attack unless given an order directly from higher up Government positions.

Lastly, using past cyber attacks and their metadata can help companies and different government departments prevent some of these different attacks on US based networks. One way to do this is to look back through case studies, and different sets of data to examine what, how, and why these attackers are getting into the systems. As well as finding out a solution to the hacks. Our target-specific recommendations differ based on the key players and variables involved in each situation, but we have identified a common thread in these recommendations, overall, we propose that the United States Government will have to take proactive action in order to prevent hostile cyber-attacks [2].

In 2020, there are already different types of cyber-attacks that network administrators need to be aware of, cloud vulnerability, AI-enhanced cyberthreats, AI Fuzzing, Machine Learning Poisoning, Smart contract hacking, social engineering attacks, and deep fakes are all new ways that attackers are trying to use to gain access into these systems. Using past data and trends to evaluate these past attacks can help determine the likelihood that an attack of that type can infiltrate and infect the systems. Using the previous trends and solutions that have been found to fix these problems can create a preventative defense for the network, creating security measures that focus on these past attacks that have been studied and evaluated.

Figure 3 shows a five-year statistical review of the different cyber-attacks faced by New Zealand during the period of 2012-2016. In the figure it can be seen that the New Zealand people were subject to more social engineering attacks and phishing attacks more than any other type of Cyber-Attacks during that time period. In 2016, the percentage of social engineering attacks and phishing attacks was more than 60% of the overall cyber-attacks in the New Zealand financial sector. Even though social engineering techniques targeted individuals, the real focus of this assault was the organizations the individuals where affiliated with [6].

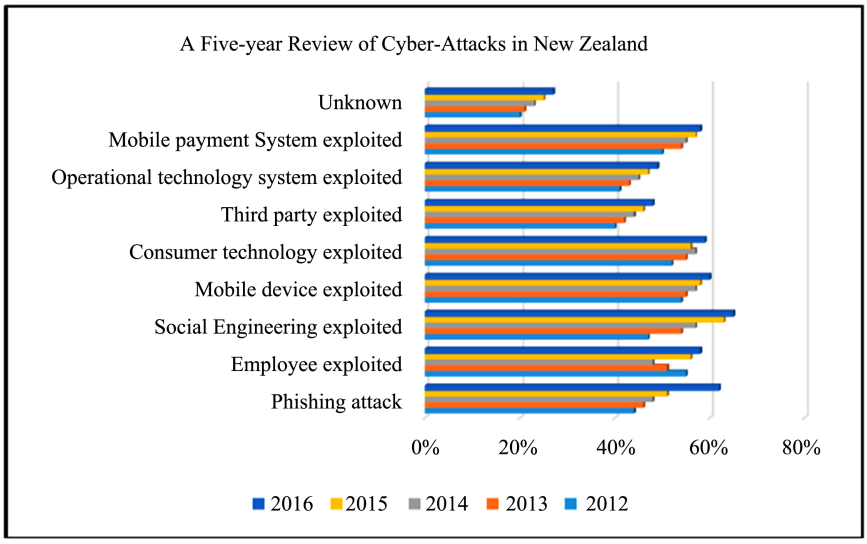

Figure 3. Cyber attack rates in new Zealand.

Using the data shown in the chart and past data from any other research that is available at the time can help improve the Cyber Security framework by understanding the attacks that are most likely to be executed on the system. This can create a preventative framework for a network to help protect from the common and general trends of Cyber-Attackers, and can help keep Network Administrators prepared for the most common attacks.

4. Conclusions

Network security is a major player in the foundation of up-and-coming companies as well as a major provider for many consumers across each and every continent and country. Ensuring that the networks that consumers do their day-to-day business on are safe and secure needs to be a primary focus of company's project management plans. Creating a plan or a structure that network administrators follow to protect and safeguard the networks that consumers use is a simple and preventative way to protect cyber systems.

By using Wu's structure of identifying sets of risks, determine relevant risk factors, establish full set of controls, and specify the methods necessary to implement, following this guideline can increase the quality of life in the IT departments of each company, by reducing the time it takes to create solutions to the network's problems, as well as making it easier for the technicians to complete more jobs at a higher frequency.

Adding to Wu's strategy, if the US government attempted to focus on creating a division of contractors and IT experts to help protect and safeguard US based networks by hitting back at them and creating more problems for the hackers before they can get to the valuable information. This can be done by creating a branch off of the Department of Homeland Security and creating a team of experienced contractors that have dealt with these types of hack back problems before.

Finally, the creation of graphs of past historical data from cyber-attacks, using things like type of hack, time of hacks, duration of the hacks, origin of the hacks, and what software was used, creating these graphs can help network administrators come up with a preventative outlook on what attacks are most commonly taking place at the time, and how they properly can prepare if one does infect the networks.

There will never be a set-in stone type of way to solving these hacks on networks due to the nature of information technology because software and methods are ever changing, it is impossible to set up a permanent framework to defend against attacks. But by using these options there can be a preventative framework in place so that when an attack happens, the network administrators and IT technicians are not surprised by it and have the means already in place to solve the issues.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Jarvenpaa, S. and Ives, B. (1994) The Global Network Organization of the Future: Information Management Opportunities and Challenges. *Journal of Management Information Systems*, **10**, 25-57. https://doi.org/10.1080/07421222.1994.11518019

[2] Rabkin, A. (2016) Enhancing Network Security. American Enterprise Institute, Washington D.C.

[3] Straub, D. and Welke, R. (1998) Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, **22**, 441. https://doi.org/10.2307/249551

[4] Wu, Y. (2020) Developing a Taxonomic Framework of Security Methods for Security Management and Information Resource Management. *Journal of Strategic Security*, **13**, 64-77. https://doi.org/10.5038/1944-0472.13.2.1787

[5] Itai, B., Louis, D., Kathryn, D., Rodrigo, O. and Ariel, S. (2016) World House Student Fellows 2016-2017 Prevention in the Cyber Domain. Perry World House University of Pennsylvania, Philadelphia.

[6] Airehrour, D., Nair, N. and Madanian, S. (2018) Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model. *Information*, **9**, 110. https://doi.org/10.3390/info9050110