Protecting the Systems that Protect Society

Brevin Parrish

Old Dominion University

Abstract

Cyber-technology has been rapidly growing around the world in the last ten years. It's impact on the life of individuals has been complex. A lot of updated communication systems, transportation systems, and security systems can be attributed to the growth of cyber-technology. The purpose of this paper is to analyze the potential ways society can protect cyber-technological systems. In this paper, there are three proposed tiers of protection. The first level of proposed protection is a do it yourself system. Individuals are challenged to effectively protect their computer systems using protection software, and ensuring that authorization keys are established. The second tier is composed of policies and authorization keys established and implemented by organizations to protect the systems of their business. Furthermore, organizations should ensure that policies are ethical, legal, and understand that predictive knowledge is slowly becoming less useful in decision making. The third proposed tier system is the criminal justice system. The first to tiers must collaborate with the first tiers to understand the type of attacks being performed on computer technology. It is essential for us to protect the computer systems that protect us on a daily basis. Cyber-technology has done numerous things to facilitate our lives, it is our job to protect it.

Introduction

Technological systems have rapidly changed the world we live in. Its parts, mechanisms, and software's may be complex, but on the surface its impact on the different aspects of life are fairly simple. The development of computer systems has allowed us to increase the effectiveness of implicated security, increase the effectiveness of our communication, and increased our safety. Before the age of technological innovation, individuals typically hid confidential documents in inconspicuous areas. Important documents were exposed to potential dangers from the elements. Things such fires, and flood destroyed those documents leaving individuals in tough positions. However, numerous factors pose a threat to the safety of our computer systems

in the present day. Cyber attacks have increased in the last decade of the technological age. Individuals have attacked computer networks compromising confidential information and the integrity of computer systems. There is no doubt in my mind that computers are a prevalent reason that the safety of society as increased. Though many may argue that it has also decreased our safety in some respects, overall computers have protected us. I propose a three-step tier system, that can effectively and cohesively band together to protect the systems that protect us.

Monitoring Usage and Access (Self-regulation Tier 1)

Society must take the necessary steps to ensure the security and confidentiality of the information stored on our computer systems. There are many ways to ensure the safety of our computer systems. One of the first steps in ensuring the safety of our computers is the purchase of malware protection software. Systems such as Firefox, and Avast ensure that malware viruses cannot attach to the functions of the computer systems. Most software protection systems come with affordable monthly payment plans or are virtually free. This means that a vast majority of people are able to purchase them and increase the security of their everyday computer systems. In addition, we should monitor the internet websites we are utilizing. There are numerous websites and browsers that carry encrypted files and information. For example, using proxy sites to watch free movies would not be ideal. Proxy sites often carry viruses that integrate themselves into the computers hardrives. This is an easy way for viruses and malware to attack and damage computer systems decreasing the security of our information. Computer systems also come with features within the settings that allow us to monitor what websites are accessible. For example, parental control is a feature used to monitor what websites children can access while working or using computer systems. We should take advantage in the implemented systems and use it to its full advantage.

There are additional precautions individuals can take to ensure that their computers are safe. Authentication is one of the biggest protection features an individual can use. Authentication is the process of using passwords or pins to verify that a user has been authorized to use the device. Authentication comes in many forms. Individuals can use fingerprints, facial recognition, and even smart cards to guard their computers from unauthorized usage. Individuals should ensure that that the passcodes they install on their computers are strong passwords. Most systems define a strong passcode as a code with between eight to twelve characters. Authorization goes hand in hand with authentication. As stated, it only allows individuals with approved access to access information that is held on the computer. This ensures that individuals won't have the authority to place viruses on the computer systems using external drives. It is also a way to monitor what is being done on the computer system. Our computer systems are some of the most important things to us. There are simple steps to ensure that our computers systems are safe and protected. Leakage of confidential information is increasing every day. It is essential that we take the necessary steps listed above, along with others to protect the systems that protect us.

Policies for Protection (Organizational Tier 2)

The implementation of cyber-technical systems has increased within organizations in the last decade. Major businesses and organizations have made it their duty to protect their computer systems. However, the issue is that predictive knowledge is becoming less useful to organizations. Due to the rapid growth in technological innovation it is difficult for working individuals to develop policies and infrastructure using predictive knowledge and predictive learning systems. The birth of new systems makes in difficult, because previous policies that have been put in place to protect the individual consumer must be amended as rapidly as the

growth of the new systems. Numerous policies within organizations or business markets have complex policies regarding cyber-systems and networks. Most policies put in place have confidentiality statements regarding the protection and use of specific information. In addition, policies layout who has authorization to the cyber systems in use. Organizations have to take another approach for developing cyber policies to protect their computer systems.

The best approach to developing cyber-policy and infrastructures in the future is ensuring that every policy idea that is brought to the table is ethical and legal. This allows organizations and businesses to create simpler, but safe policies regarding the cyber systems. For example, every year a new Apple Iphone is released. The terms and conditions do not typically change. They have simple statements in place that are not only ethical, but legal and ensure the protection of their consumers. Businesses should take the same approach of making a layout of policy that is ethical and legal from the beginning. Then when the boom of technological innovation occurs again, companies will be able to add new terms or policies to the bottom of the template they created before. Predictive knowledge and learning systems have been a great resource for companies to use throughout business ventures. However, it is impossible to say that the predicted situations will occur. Therefore, it is the job the organizations and businesses to be on their toes and ready for anything that may occur.

Preventing Cybercrimes (Criminal Justice Protection Tier 3)

Cybercrimes have become more prevalent in today's society over the past decade. Hackers are becoming a predominant threat within the cyber community. Traditional crimes such as fraud, embezzlement, and scamming typically occurred in face to face transactions. However, due to the technological innovation of computer systems, crimes are now able to be performed digitally. There are numerous cases where individuals used personal desktops and even cell

phones to launder money from individuals. Criminal justice is needed now more than ever. Criminal justice would be the third tier of protection for our computer systems. In order to effectively protect us they will need the help of society and the help of organizations to learn what types of crimes are being performed. They also need to understand how the crimes are being performed and how they can assist us in stopping them from reoccurring. Computer systems protect our law enforcement officers and government officials. The complex security systems are generated through desktops and other forms of technology. In order to ensure that the computer systems are effectively doing their jobs, our criminal justice systems must protect the computer systems that protect them.

Conclusion

Over the last decade computer systems have facilitated in the everyday life of individuals. It has minimized the complexity of numerous activities performed on a day to day basis. They have increased the effectiveness of our communication, the effectiveness of our security, and has in ways increased our safety. It is essential that we take action in protecting the technological systems that protect us every day. Individuals have to take the necessary steps to protect their computer systems. They can simply monitor the websites they use, purchase protection software, and ensure the authorization of every user. Policies need to be thoroughly amended to protect the computer systems in use. Authentication and authorization policies should be laid out so that individuals know there is zero tolerance for unauthorized usage of computers. Lastly, the top two tiers should work diligently with our criminal justice system to stop the hackers and other attacks on our computer systems. It is essential that each tier takes the necessary steps to protect the cyber-technological systems we use every day.