Multi-Knowledge Electronic Comprehensive Journal for Education and Science Publications (MECSJ)
ISSUE (32), May (2020)
ISSN: 2616-9185
www.mecsj.com

The Role of Cybersecurity to Protect our Information

Ali Alasmari
Doctoral student in Cybersecurity at Marymount University
E-mail: Ali_moon1981@yahoo.com

Abstract

Cybersecurity covers all measures that are implemented in the application of online services to ensure sufficient protection of information from potential attacks and compromise. It involves systems that are designed to protect and secure computer systems, networks, and programs from cyber-attacks. The primary aim of cybersecurity is to maximize the confidentiality of private data and ensure the integrity of computer networks and systems. The study aimed at exploring the role of cybersecurity in protecting personal information and limiting possible cyber attacks that might lead to huge financial and technical losses for organizations, governments, and individuals. The study addresses the goal by reviewing previous literature on cybersecurity measures and examples of targeted attacks that have been recorded in recent years. Based on the findings, the cybersecurity measures that are commonly adopted in organizations include the installation of malware defenses, controlled use of managerial authorization, auditing of logs, and continuous system monitoring. The measures ensure that information is protected from potential attacks. Continuous monitoring of systems helps identify unusual events on the networks. Controlled use through managerial authorization is also critical towards the protection of personal data from potential attacks. The adoption of these measures is essential in providing cyber defenses. They also protect data, systems, and networks from attacks. The measures guarantee internet users, whether individuals, organizations, or governments' privacy and safety of private information. The inclusion

of cybersecurity in modern world politics can also help in the formulation of policies that enhance the safety and privacy of personal data in cyberspace. Cybersecurity is equivalent to national security, and it is for this reason that governments take an international approach in protecting their activities in cyberspace.

Keywords: Cybersecurity , information security , organizations, cyber attack.

الملخص:

يشمل الأمن السيبراني كافة التدابير اللازمة التي يتم تنفيذها في تطبيق الخدمات عبر الإنترنت لضمان الحماية الكافية للمعلومات وامنها من أي هجمات محتملة من قبل مجرمي الحاسب الالي (الهكر). ويتضمن أنظمة مصممة لحماية وتأمين أنظمة الكمبيوتر والشبكات والبرامج من الهجمات السيبرانية.

فالهدف الأساسي للأمن السيبراني هو تعزيز سرية امن البيانات الخاصة وضمان تكامل شبكات وأنظمة الكمبيوتر. وهدفت الدراسة إلى استكشاف دور الأمن السيبراني في حماية المعلومات الشخصية والحد من الهجمات السيبرانية المحتملة التي قد تؤدي إلى خسائر مالية في تقنيتها الضخمة للمنظمات والحكومات والأفراد.

وتتناول الدراسة الهدف من خلال مراجعة الأدبيات السابقة حول تدابير الأمن السيبراني وأمثلة على الهجمات المستهدفة التي تم تسجيلها في السنوات الأخيرة. استنادًا إلى النتائج، والتي تشمل إجراءات الأمن السيبراني التي يتم اعتمادها بشكل شائع في المؤسسات لتامين والدفاع عن البرامج الضارة، والاستخدام الخاضع للرقابة الإدارية، ومراجعة السجلات، والمراقبة المستمرة للنظام. وتضمن التدابير حماية المعلومات من الهجمات المحتملة. وتساعد المراقبة المستمرة للأنظمة على تحديد واكتشاف الأحداث غير العادية على الشبكات.

فالاستخدام الخاضع للرقابة من خلال التفويض الإداري أمر بالغ الأهمية أيضًا لحماية البيانات الشخصية من الهجمات المحتملة. ويعد اعتماد هذه التدابير اللازمة أمرًا ضروريًا في توفير الامن السيبراني. كما أنها تحمي البيانات والأنظمة والشبكات من أي هجوم يستهدفها. وتضمن هذه الإجراءات مستخدمي الإنترنت، سواء أكانوا أفرادًا أو منظمات أو شركات خاصة او حكومات ولضمان امن معلوماتها الخاصة بها.

إن إدراج الأمن السيبراني في السياسات العالمية الحديثة يمكن أن يساعد أيضًا في صياغة السياسات التي تعزز سلامة وخصوصية البيانات الشخصية في الفضاء السيبراني. فالأمن السيبراني يعادل الأمن القومي، ولهذا السبب تتخذ الحكومات نهجًا دوليًا لحماية امنها وأنشطتها في الفضاء السيبراني.

الكلمات المفتاحية: الامن السيبراني ، امن المعلومات ،الشركات ، هجوم سيبراني .

The Role of Cybersecurity to Protect our Information

Introduction

The modern world is now more dependent on information than ever before (De Bruijn &Janssen, 2017). In fact, companies that control information across the globe are the ones that make huge profits as people seek data to conduct business and grow the economy. The personal space has now been merged with cyberspace, where people have access to the internet, smartphones, and other digital gadgets (De Bruijn & Janssen, 2017). The amount of information shared on the internet is unprecedented. Business conduct transactions online, the government run digitally, and individuals also depend on cyberspace to run their daily activities (Goutam, 2015). People who shared information online tend to underestimate the threats that underlie such activity and tend to believe that the internet is safe and secure. However, with the continued reliance on cyber activities, criminals have found a way to infiltrate the internet and take advantage of the loopholes to either steal or manipulate data (Gercke, 2012). Cybercrime is a rising evil that people will have to contend with as long as the cyberspace remains open to all people (Gercke, 2012). That is why it is important to implement cybersecurity measures that are able to prevent or mitigate the effects of cybercrime as well as protect sensitive information. Hence, the major role of cybersecurity is to secure information and make the internet a safe space.

The major reason why cybersecurity is needed in the world today is because of the increasing cases of cybercrime (Buch, Ganda, Kalola, & Borad, 2017). Cybercrime entails all the illegal activities that take place on the internet, which include hacking; theft of private information and data; theft of financial transfer passwords and credit card fraud; illegal acquisition of digital property; general disturbance of networks such as virus installations, phishing, spamming; cyberstalking; and piracy (Buch, Ganda, Kalola, & Borad, 2017). For example, in the United States, data threats and breaches have become rampant. For instance, in 2017 alone, there were over one thousand recorded data breaches, amounting to the exposure of over one billion records on delicate information (Ablon, 2018). There are black-markets on the internet where cybercriminals peddle

stolen data (Ablon, 2018). In hindsight, all sectors of the economy are vulnerable to cybercrime from banking institutions, retail stores, healthcare organizations, governmental institutions and the entertainment industry (Ablon, 2018).

Usually, cyber attackers are motivated by varied reasons, and such they are made up of different categories, namely, cyber terrorists, state-sponsored, hacktivists, and cybercriminals (Ablon, 2018). Cyber terrorists are usually, extremists, motivated by political reasons and aiming to cause fear, harm or prove their cyber power (Ablon, 2018; Tsakanyan, 2017). State-sponsored players breach the internet solely because they are funded by a state to advance their own national interests (Ablon, 2018; Tsakanyan, 2017). Hacktivists are internet activists who seek to shine a light or rebel against a certain actions, mostly motivate for political, social, and economic or even human rights courses (Ablon, 2018). Lastly, cybercriminals are motivated by the money they make from selling stolen data on black-markets (Ablon, 2018; Tsakanyan, 2017). It is the existence of a wide network of cybercrime that necessitates the implementation of cybersecurity measures.

Importantly, it is worth noting that these cybersecurity threats are not just abstract but have been experienced since the inception of the digital footprint. Buch, Ganda, Kalola, & Borad (2017) have recorded that the first cybercrime occurrence was experienced as early as 1820; the first mail spam occurred in 1978, and in 1982 Apple reported the first virus which was installed on its computer. Viadya (2015) surveyed the major cyber-attacks that took place between 2001 and 2013, and reported that within this time, there were several targeted and undirected that attacks that cost various institutions billions of money. Among the myriad undirected attacks were the 2003 *Slammer* virus that instigated the collapse of routers and the 2004 *Mydoom* worm that originated from Russia and led to a loss of over thirty-eight billion dollars (Viadya, 2015). Viadya (2015) also reported several targeted attacks directed at states, including the 2009 attack that was directed towards Israeli government institutions. Some of the companies that have been the subject of attack in recent years include TJX in 2007, Citibank cyber-attack in 2009,

and Google in 2010. All these examples show, especially, large companies are vulnerable to cyber threats and attacks due to a lack of cybersecurity measures (Viadya, 2015).

However, the most noteworthy cyber-attack in recent history is the one directed at Sony Pictures Entertainment by the Guardians of Peace group in 2014 (Sanchez, 2015). This well-orchestrated hack on Sony brought the entire company to a halt. The Guardians of Peace claimed to have accessed over one hundred terabytes of data which contained employee private information, movie scripts, and employee social security numbers (Sanchez, 2015). A few days after the hack, the hacker group posted the information online and made its demands, which included a requirement that Sony was not to release a movie by the title, *the Interview* (Sanchez, 2015). It is after this very damaging hack that organizations started looking at ways to prevent cyber-attacks. Sanchez (2015) suggests that a few cybersecurity measures such as the installation of malware defenses, constant monitoring of the system, controlled use of managerial authorizations, and audit logs could have prevented the hack or mitigated the damage. Hence, the role of cybersecurity in organizations cannot be overemphasized enough.

Simply stated, cybersecurity entails all the measures that are taken during the usage of online services to ensure that online information is protected. It is a collection of technologies "designed to protect and secure networks, computer systems, various programs and data from cyber-attack, damage all these things or unauthorized access these" (Buch, Ganda, Kalola, & Borad, 2017, p. 18). The main aims of cybersecurity might include to ensure confidentiality of sensitive information and to protect the integrity of computer systems and networks. Major problem areas to cybersecurity include viruses, worms, and hackers (Buch, Ganda, Kalola, & Borad, 2017). In most instances, it is extremely difficult to control cyber activities because cyberspace is virtual, and people sometimes operate without digital identities (Goutam, 2015). Some of these people aim to use cyber threats such as viruses to make others vulnerable.

Goutam (2015) argues that cybersecurity in the present world is only considered important for private persons and families but also to institutions and businesses. Cybersecurity is important because it provides appropriate cyber defenses and provides

protection of data and information (Buch, Ganda, Kalola, & Borad, 2017). Besides, cybersecurity also protects the systems and networks from attacks as well as private information. Internet users are accorded the privacy they need and deserve from the application of cybersecurity strategies. However, despite the apparent need for cybersecurity, the world is still slow in implementing reasonable measures to avoid data breaches. In fact, the United States still remains the highest target for cyber-attacks (Rawal, Eberhard & Lee, 2016).

Additionally, the time taken to repair or resolve vulnerabilities from cyber threats is very long. A research conducted by Rawal, Eberhard & Lee (2016) revealed that Google, for instance, took two months to repair vulnerabilities and bugs took three to four months to patch. Cyber attackers take less time to penetrate a system, and as such, organizations need to be vigilant and adopt better cybersecurity measures.

In arguing in favor of preventive cybersecurity measures, Barsade, Davis, Dura, Ornelas, & Smith (2011) suggested a five-stage model that the course cybersecurity activities take. These stages are; prevention, preemption, halting, mitigations and retaliation (Barsade, Davis, Dura, Ornelas, & Smith, 2011). At the prevention phase, the main aim is to avert an attack by the cyber reinforcement defenses and to reduce security risks. The preemption stage comes in when it an attack is imminent. It entails taking measures to impede the attack from occurring by the use of threats, preemptive strikes, or even diplomacy (Barsade, Davis, Dura, Ornelas, & Smith, 2011). The halting stage takes place when an attack is ongoing, and the measure is to ensure that the same comes to a stop. In the mitigation stage, the actors ensure that the damage is controlled, and no more loss of data is occasioned by conducting risk assessments (Barsade, Davis, Dura, Ornelas, & Smith, 2011). The last stage is the retaliation stage, which involves the victim of the attack or relevant authorities imposing punitive measures to dis-incentivize the attack (Barsade, Davis, Dura, Ornelas, & Smith, 2011). Usually, measures such as economic sanctions and retaliatory attacks are used. Care should be taken at this stage, not to aggravate the situation.

Internationally, the role of cybersecurity has also been heavily recognized in modern world politics. Nations, especially superpowers, use the strength of cybersecurity to flex their muscles and advance national interests (Tsakanyan, 2017). Most nations now consider cybersecurity as part of their national security (Tsakanyan, 2017). For instance, the United States being a world leader in information technology, it is both a victim and a strong bargainer in international politics (Tsakanyan, 2017). That is why cybersecurity is controlled by the military. In the case of China, it considers cybersecurity to be equivalent to national security (Tsakanyan, 2017). In this regard, software that emanates from the West is restricted in China. The internet and digital platforms are highly regulated by the state in China (Tsakanyan, 2017). Generally, no single approach can be attributed to how states operate cybersecurity, as each has its ways; but it is evident that cybersecurity is so important to nations in the present world. However, with states debating on whether to use a domestic military approach towards enforcing cybersecurity or not, O'Connell (2012) suggests that cybersecurity should be viewed in the preview of international law and be controlled by international standards.

Despite the reasons outlined in favor of implementing cybersecurity, Odlyzko (2019) argues that cybersecurity is not important. Odlyzko (2019) states that the world is in a state of hysteria about cybersecurity and has blown some threats out of proportion. According to Odlyzko (2019), there has been no major digital catastrophe and that the world is doing well as far as the cyberspace is concerned. On another note, Nojeim (2012) has cautioned that unchecked implementation of cybersecurity might threaten people right to privacy and curtail their liberties. Hence, while dealing with cybersecurity strategies, it is important to ensure that the right to privacy and civil liberties of internet users are not infringed.

In the end, as long as the cyberspace exists, so will threats to information, cybercrime and so will be a need for cybersecurity increase. Many people are ignorant and do not know about the threats on the internet, but only look at the internet as a safe space that can be accessed daily (De Bruijn & Janssen, 2017). Hence, there is a need to create awareness and encourage people from individual levels to understand the risks that

come with internet use, to implement protective measures (De Bruijn & Janssen, 2017). Information is power, and if left in the wrong hands, it can be used as a weapon, just like any other physical weapon.

Conclusion

Cybersecurity is increasingly becoming relevant, particularly with the rising cybercrime in the modern world. Recent technological advancements have seen a significant increase in the use of the internet, smartphones, and other digital gadgets. The amount of information that people are sharing on the internet is unprecedented. Businesses, governments, and individuals are finding the technologies more relevant in completing daily transactions, activities, and delivery of services. However, with the expansive use of information technology comes significant risks and threats. The threats range from hacking, theft of private information, illegal acquisition of digital property, network disturbances, spamming, phishing, piracy, and cyberstalking. The existence of wide networks of cyber threats that necessitates the adoption of cybersecurity measures at different levels.

The study aimed at exploring the role of cybersecurity in protecting information stored on digital platforms. The findings indicate that the lack of elaborate cybersecurity measures has led to huge financial losses. For example, the 2004 *Mydoom* worm that originated from Russia resulted in a loss of over $30 billion in the US. Targeted attacks on government infrastructure create interruption and loss of important information. The huge losses reported in recent years from cyberattacks make cybersecurity measures critical in the protection of private information. Some of the cybersecurity measures identified in the study include of installation of malware defenses, controlled use of managerial authorizations, continuous system monitoring, and audit logs. The measures are important prevention of potential attacks and limiting the extent of damage to critical infrastructure. The installation of malware defenses protects against virus and malware attacks on technological systems and structures.

References

Ablon, L. (2018). *Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data*. RAND.

Barsade, I., Davis, L., Dura, K., Ornelas, R., & Smith, A. (2011). Prevention in the Cyber Domain. *RUSI Journal*, *156*(2), 22-27.

Buch, R., Ganda, D., Kalola, P., & Borad, N. (2017). World of Cyber Security and Cybercrime.

De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1-7.

Gercke, M. (2012). *Understanding Cybercrimes: Phenomena, Challenges and Legal Response*. International Telecommunication Union.

Goutam, R. K. (2015). Importance of cyber security. *International Journal of Computer Applications*, *111*(7).

Nojeim, G. T. (2010). Cybersecurity and Freedom on the Internet. *J. Nat'l Sec. L. & Pol'y*, *4*, 119.

O'Connell, M. E. (2012). Cyber security without cyber war. *Journal of Conflict and Security Law*, *17*(2), 187-209.

Odlyzko, A. (2019). Cybersecurity is not very important. *Ubiquity*, *2019*(June), 2.

Rawal, B. S., Eberhardt, G., & Lee, J. (2016). Cybersecurity snapshot: Google, twitter, and other online databases. *Journal of Advanced Computer Science & Technology*, *5*(1), 14-22.

Sanchez, G. (2015). Case study: Critical controls that Sony should have implemented. *SANS Institute*.

Tsakanyan, V. T. (2017). The role of cybersecurity in world politics. *Vestnik RUDN. International Relations*, *17*(2), 339-348.

Vaidya, T. (2015). 2001-2013: Survey and Analysis of Major Cyberattacks. *arXiv preprint arXiv:1507.06673*.