Report

[Author Name]

[Institutional Affiliation(s)]

Report

**Introduction**

Due to the rise in technologies, many companies are incorporating new technologies to make their systems efficient. However, despite the emergence of new technologies one issue that all the organizations are facing is a security issue. Systems are vulnerable to security threats due to which it is necessary to address the cybersecurity issue. Due to which the executive team of our media company decided to make a team whose responsibility was to address security issues. While working on the security of the systems our team decided to replace IPv4 to IPv6 while also implementing a smart security system based on IoT. However, while integrating and implementing this strategy, several issues were encountered. This report will discuss the issues that occurred during implementing the smart security system based on IoT. Also, the requirements and future recommendations that needed to be addressed to make the systems more secure is also discussed.

**Body**

When the executive team of our company recognized the importance of cybersecurity, they assigned us the task to develop a strategy that includes a security plan needed to protect the company’s data. For this purpose, we divided the task among the team and developed a security plan. Firstly, we decided to replace IPv4 to IPv6 because it offers a large pool of IP addresses. It can also run end to end encryption while supporting secure name resolution (Kim & Paek, 2017). This also helps in reducing ARP poisoning and several naming attacks. Thus making the system more secure. Additionally, using just IPv6 does not solve the security issue and there is a need to make a proper security system. For this purpose, a smart security system based on IoT was developed. The system is capable of generating alarms and taking intelligent decisions using IoT concepts. It uses both Bluetooth and GSM technology that will help in managing the organization from both indoor and outdoor. The system also uses various sensors such as motion, gas, and laser making it more flexible (Saifuzzaman & Nur, 2017).

After developing the security system next step was its integration with other systems and its implementation in the organization. However, while implementing and integrating new systems several issues were faced. The first issue that we faced was shifting from IPv4 to IPV6. As IPv6 is new therefore it is not compatible with systems using IPv4. Also, it requires new server software and equipment thus making its deployment a bit expensive. Specifically, discussing about LAN (local area network), it contains less than 50 addressed devices due to which there is no need to use more than a billion new LAN addresses as it is a wastage of resources. Additionally, the current operating systems and routers provide less support for IPv6 and therefore needed to be updated. Also, major ISPs offer some IPv6 functionality yet still they need improvement. However, there are certain methods such as 6 to 4 that can be useful in transitioning from IPv4 to IPv6 (Wu & Metz, 2012).

Moving on towards the smart security system, several issues occurred while implementing this system as well. The issue was that connecting wire to deploy the system is itself one of the most hectic tasks. Also, as smart security systems use several sensors so maintaining the sensors regularly is very necessary as sometimes the sensors stop working due to several issues. This will again cause a problem as without sensors the detection of the potential threats is not possible. Additionally, sensors require more voltage that can increase the power issue. This issue will, in turn, result in internet connection fluctuations. Also, in case of any intruder detection SMS will be sent to the respective person of an organization responsible for security. As low power and the range of wireless are traded off by lowering bandwidth. The SMS requires a maximum wireless range that may increase bandwidth issues. Moreover, to integrate the new system with the existing security software is also an issue because existing software is based on old cryptographic techniques. On the other hand smart security system software uses the latest techniques by incorporating several mini techniques such as GSM and Bluetooth.

The deployment of several latest technologies does not only affect older technologies but it influences people working with older technology as well. Most of the people in the company were trained to use older software for security so for them, a smart security system that is based on IoT was difficult to understand. Also, transitioning from IPv4 to IPv6 will cause more problems for the employees. Many servers and routers do not support IPv6 and most of the sites use IPv4. So making a connection through IPv6 between router and device that supports IPv4 is not easy (Levin, S& Schmidt, 2014). Thus due to the implementation of new techniques hiring new employees is a major necessity. This will cause more issues as hiring new employees and training requires lots of effort. Also, a smart security system based on IoT can accommodate several new technologies so hiring new people for every new technology is difficult. Additionally, data governance issues will arise due to the deployment of a new security system. So there is a need for the governing body that defines a set of rules and procedures that will help in ensuring the integrity and security of the newly deployed system.

**Conclusion**

Cybersecurity is a major issue that needs to be addressed. There are several benefits of IPv6 and smart security systems based on IoT. However, deploying any new technology can be difficult as several issues rise with it. There are lots of software that can help in the transition from IPv4 to IPv6, yet incorporating the use of IPv6 with older technologies is difficult. Additionally, the smart security system also has certain limitations, yet it is a flexible system that can accommodate several new technologies. Also, most people are not familiar with the latest technology. It is, therefore, necessary to train people before deploying new technology so that they can also utilize the benefits of new technology.

**References**

Kim, H. S., Ko, J., Culler, D. E., & Paek, J. (2017). Challenging the IPv6 routing protocol for low-power and lossy networks (RPL): A survey. *IEEE Communications Surveys & Tutorials*, *19*(4), 2502-2525.

Levin, S. L., & Schmidt, S. (2014). IPv4 to IPv6: Challenges, solutions, and lessons. *Telecommunications Policy*, *38*(11), 1059-1068.

Saifuzzaman, M., Khan, A. H., Moon, N. N., & Nur, F. N. (2017). Smart Security for an Organization based on IoT. *International Journal of Computer Applications*, *165*(10), 33-38.

Wu, P., Cui, Y., Wu, J., Liu, J., & Metz, C. (2012). Transition from IPv4 to IPv6: A state-of-the-art survey. *IEEE Communications Surveys & Tutorials*, *15*(3), 1407-1424.