Critical Elements of a Vigilant Cybersecurity Response Plan

Ashish Yadav
Department of Computer Science & Information Technology
CERT, India

Abstract— Incident response is the technique (science) of responding to cyber security-related breaches. That's why preparing effective Cybersecurity response plan has to be on the top priority for all organizations, regardless of strength and size. Here some of the critical elements to which consider when building such type strategies or plans.

Key words: Cybersecurity

I. Introduction

A. *Problem*

The cyberattacks increasing annually, organizations should be ready and secure. To find those elements that affects Cybersecurity response plan, those elements should be the top most priority for all digital structure or organization.

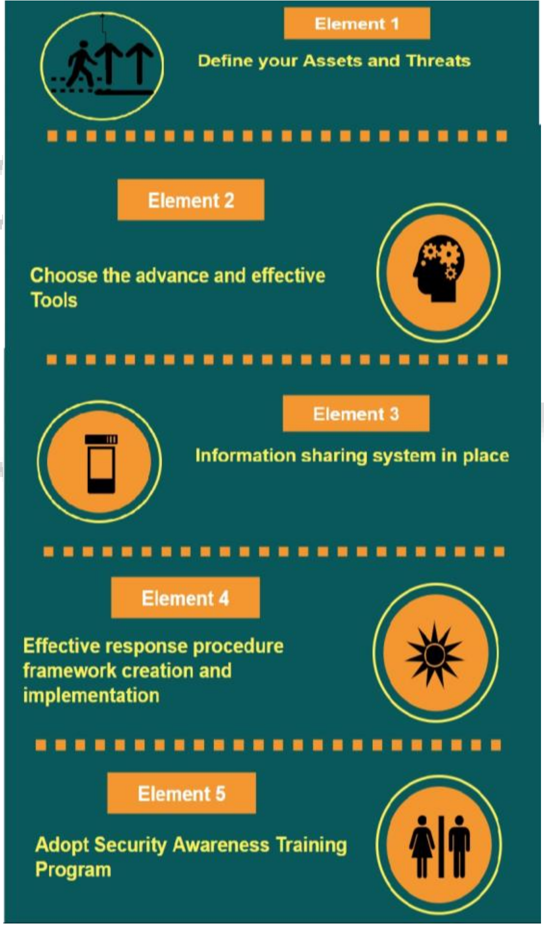
Element 1
Define your Assets and Threats
Element 2
Choose the advance and effective Tools
Element 3
Information sharing system in place
Element 4
Effective response procedure framework creation and implementation
Element 5
Adopt Security Awareness Training Program

Fig. 1: Critical Elements of a Vigilant Cybersecurity Response Plan

B. *Many Cyber Security Experts Agree*

This is the time to get serious about cyber security incident response. The cyber security incident response plan is your path for responding to a Cybersecurity attacks. A cyber incident response plan needs several key core elements to be effective.

To ensure your plan is applicable and it should include at least following 5 main elements.

II. Define Your Assets & Threats

Identify the financial and information assets that are important to your business and technology that you rely on. When developing a Cybersecurity incident response plan, you need to know what assets you are protecting and the inherent value or cost of those assets and define how they secure. These assets could include essential data include third party data and vendor data, network access, an accounting system; LAN files records, digitally stored business documents and more.

III. Choose the Advance & Effective Tools

Attacker and malicious personals are using the most updated and advanced technology. It is important to keep up with the latest technologies as to stay updated and safe. Cybersecurity threats are not only increased but have also become more refined. A major challenge in combating these threats is lack of Cybersecurity experts that can keep up with new technology, including whether forensic evidence gathering is required which is important in mitigating attacks. So the of your Cybersecurity incident response plan based on your effective Cyber security tools which safeguarding your IT infrastructure from Hackers, viruses, malware and phishing etc.

IV. Information Sharing System in Place

No organisation or system is immune from attack, Involve in the periodically sharing of reliable, actionable Cybersecurity fruitful information with internal and external entrepreneur (including entities and public authorities within and outside the financial division) on risk, threats, vulnerabilities, incidents, and responses to improve defences, control damage, increase circumstantial awareness, and deep learning.

V. Effective Response Procedure Framework Creation & Implementation

Establish and maintain a Cybersecurity procedure and framework adapted to specific Cybersecurity risks and properly informed and complying by international, national, and industry standards and rules or guidelines. Which appropriately assess the nature, scope, and impact of a Cybersecurity incident, contain the security incident and mitigate its impact? Communicate internal and external allies or partners (such as law enforcement, regulators, and other public authorities, as well as third-party service providers, and customers and coordinate additional response activities as required.

VI. Adopt Security Awareness Training Program

Organizations are concerned and constantly on the looking for ways to best protect their data and infrastructure from being attack or compromised. Cybersecurity threats and vulnerabilities growing expeditiously, Learn the best practices and technical standards to treat them. One of the solutions to do this is to implement a Cybersecurity Awareness Training for their workers.

VII. SOLUTION

All organisations need a flexible and vigilant Cybersecurity Response Plan in order to align their Cybersecurity risks with their mitigation strategy. The better understanding of the elements helps the organization to develop effective cyber security plan ultimately, this leads to faster, and more agile and more comprehensive defences.

VIII. CONCLUSION

Every organization should have a Cybersecurity incident handling plan, which has various key elements. By integrating these key elements, organizations will have a considerable advantage over the enemies that target them.

REFERENCES

[1] http://www.crossdomainsolutions.com/cyber-security/elements/
[2] https://www.blueliv.com/blog-news/research/defining-the-key-elements-of-a-cybersecurity-strategy/
[3] https://www.bankinfosecurity.asia/interviews/7-components-for-cybersecurity-readiness-i-2949