Reduce potential vulnerabilities in Cyber Security

Name

Institution affiliated

Date

Initial post

Enhancing cyber security is an active, dynamic effort since cyber threats are always evolving. The U.S. government has in the past instituted measures to protect the critical information infrastructure, but there is always room for improvement and continuous monitoring to ensure there is an up-to-date list of cyber threats and vulnerabilities, and the measures put in place are still relevant.

In order to effectively reduce potential vulnerabilities, protect against intrusion attempts, and better anticipate future threats, there is need to continuously resource the national agencies and organs responsible for cyber security. For example, the government should continuously hire additional personnel to the Computer Emergency Readiness Team (Amoroso, 2012). The additional personnel should bring in new skills and knowledge on contemporary cyber security threats and vulnerabilities, and they should work with the experienced veterans to design and recommend better information security infrastructure.

Frequent and accurate assessment of the national information and communications infrastructure is needed to ensure these infrastructures are not only up to date, but they are also well protected with both physical and non-physical measures. Assessments should include evaluating the skills of the personnel manning these infrastructure. Information and communication staff should be well trained to detect vulnerabilities and threats. Assessments should also look at the security aspects of critical infrastructure, including where they are located and how they are physically protected from intrusion. The software used should be well secured with up-to-date firewalls.

There is need to invest in cyber security research and development. Just like many areas of national security, cyber security should be accorded the urgency in terms of funding R&D. According to Harkins (2016), cyber security team members should “research a wide range of security topics in depth.” Research is one of the most critical tools in solving current and future problems. Through research, the government will be able to not only identify future cyber threats, but also (and most importantly) come up with interventions before these threats actualize. Research will help the security team to anticipate future threats and improve current infrastructure to withstand these threats. Research will also help to expose the vulnerabilities facing the critical communications and information infrastructure. If vulnerabilities are identified and fixed, cyber security threats become less of a problem.

Cyber security can also be improved through the use of strong authentication. In the recent years, research in multi-factor authentication (MFA) has proved increasingly crucial. Various governments are already encouraging the use of MFA. However, the U.S. government has not been pushing hard for the adoption of MFA by both government offices and the private sector. MFA has proven to be efficient in improving the challenges faces by single authentication.

As Mahaffey et al. (2016) explain, password-based authentication alone cannot offer cyber security. Cybercriminals have become good at phishing and tricking users to disclose their passwords, and these are no longer safe. According to Hong (2012), phishing has more than doubled in past few years, and it has been used in major hacks including DNC, Norway security breach of government emails, as well as the recent attempt to hack the email accounts of established U.S. journalists. A host of hacking and attempts thereof in the recent past have had everything to do with phishing. Thus, government websites and other critical public service websites should be secured with MFA. In addition to passwords, for example, gaining access to government websites portals should require the use of biometrics. This is because biometrics are difficult to fake, and they are also different from every individual.

Response to posts

Post 1

Hi, I like your post. According to Janssen, Matheus & Zuiderwijk (2015), Big Data refers to data that is created from “large, diverse, complex, longitudinal, and distributed data sets” which are generated from and by multiple resources including sensors, internet transactions, user browsing, clicks, etc. In my understanding, Big Data means having a voluptuous database and systems to collect data from various online activity.

Many organizations and governments are investing in Big Data, and they are using data analysis methods to predict trends. Janssen et al. (2015) defines Open Linked Data as the opening and combination of various data sets. The concept of Big and Open Linked Data promotes better utilization of data resources. In my opinion, evidence-based policy (EBP) is one of the areas of application of BOLD. EBP is based on the idea that policy decisions should be based on evidence and rational analysis of data. Thus, BOLD should be able to provide the “evidence” needed to make public policy decisions.

Post 2

Hello, I like your post. You have talked about information security as one of the greatest functions of any organization or government, and I think you got the right ideas. In my understanding, information is power. That is why cybercriminals go greater miles to either gain access to critical information or destroy it altogether. It is for this reason that cyber security is crucial. You have also talked about SQL injection, and I agree that it is one of the most common methods used by cybercriminals to gain access to and destroy critical information. In addition to SQL injection, I think phishing has also gained attention in the recent past. Basically, cybercriminals use tricks on unsuspecting users to get access to their passwords and then use the passwords to log into servers. In phishing, cybercriminals disguise themselves as trustworthy entities to get access to user information. One of the ways to protect against phishing would be to use multi-factor authentication (MFA) and train users how to detect phishers. For example, people should be encouraged to use both passwords and biometrics to log into government portals and websites.

Post 3

Hello, I like your post. You talk of the ability of organizations to control vulnerability, and I agree with you that this is the best shot that organizations have to defend against cyber threats. In my understanding, threats cannot be a problem if an organization is not vulnerable to them. Threats only become a risk when they find entry points. This is because threats take advantage of the available loopholes to cause harm. For example, cybercriminals only succeed if they are able to phish their way into critical information. In such a case, the organization should ensure it is not vulnerable to phishing by training its staff on how to identify and mitigate phishing attempts.

In addition to the three “major cyber security activities” you have mentioned, I think it is important that an organization carried out frequent vulnerability assessments. In fact, more resources should be invested in finding the sources of vulnerabilities and sealing them than the resources used to develop cyber security strategies. This is because when vulnerabilities are minimized, there would not be need to invest in expensive counterattack measures.

References

Amoroso, E. (2012). Cyber attacks: protecting national infrastructure. Elsevier.

Harkins, M. W. (2016). Emerging Threats and Vulnerabilities: Reality and Rhetoric. In *Managing Risk and Information Security* (pp. 81-98). Apress, Berkeley, CA.

Hong, J. (2012). The state of phishing attacks. *Commun. ACM*, *55*(1), 74-81.

Janssen, M., Matheus, R., & Zuiderwijk, A. (2015, August). Big and open linked data (BOLD) to create smart cities and citizens: Insights from smart energy and mobility cases. In *International Conference on Electronic Government* (pp. 79-90). Springer, Cham.

Mahaffey, K. P., Richardson, D. L., Salomon, A., Croy, R. T., Walker, S. A., Buck, B. J., ... & Golombek, D. (2016). *U.S. Patent No. 9,374,369*. Washington, DC: U.S. Patent and Trademark Office.