International Journal of Science, Environment and Technology, Vol. 5, No 1, 2016, 95 – 101

ISSN 2278-3687 (O)
2277-663X (P)

# THREATS AND VULNERABILITY PREVENTIVE MECHANISM

**[1]A.S. Kalyana Kumar and [2]Dr. T. Abdul Razak**
[1]Assistant Professor
Department of Information Technology,
Institute of Public Enterprise - OU Campus, Hyderabad, India
[2]Associate Professor, Department of Computer Science,
Jamal Mohamed College, Tiruchirapalli, Tamilnadu, India
E-mails: [1]kalyan@ipeindia.org / [2]abdul1964@yahoo.com

**Abstract:** Vulnerability management is the most critical phase of the critical infrastructure cyber security. During the process of cyber security, the asset management would be the initial and base for the cyber security process. If we are able to identify the scope and its assets without any defect, the assessment and the expected threats also can be identify which leads the organization or any business to proactive way of risk management. In this paper we will discuss the assessing the vulnerability management process with respect to the assets and mitigating the security threat and solutions to its challenges in easy nine steps.

**Keywords:** Vulnerability, Asset, Threat and Risk management.

## 1. Introduction:

The number of servers, desktops, laptops, phones and personal devices accessing network data is constantly growing. The number of applications in use grows nearly exponentially. And as known vulnerabilities grew in number, IT managers found that traditional vulnerability management solutions could easily find more problems than could be fixed.

The cyber security and its related risks proactive or reactive combating requires assessment of the victimized assets as well as the business cost. The only way of assessing the economical loss assessment could be possible only after knowing the exact assessment of assets in the scope of the business. About 95% of breaches target known vulnerabilities. If we look at the preventive methods, risk could be calculated as Risk = Assets x Vulnerabilities x Threats.

*Received Dec 31, 2015 * Published Feb 2, 2016 * www.ijset.net*

Asset
Threat
Vulnerability

**Figure 1: Threat Asset Vulnerability in an active relation**

Here, we can do nothing on available assets because they are constant like its associated or possible threats. But vulnerabilities could be controlled to minimize the risk. To control the vulnerabilities, we need to fix in an appropriate way in right time with the help of right method.

Building an effective vulnerability management program is critical to every organization, no matter the type. Businesses must understand how to effectively prevent cyber-attacks by eliminating weaknesses in their networks. A risk based cyber security framework- a set of industry standards and best practices to help organizations manage cyber security risks.

## 2. Attack life cycle:

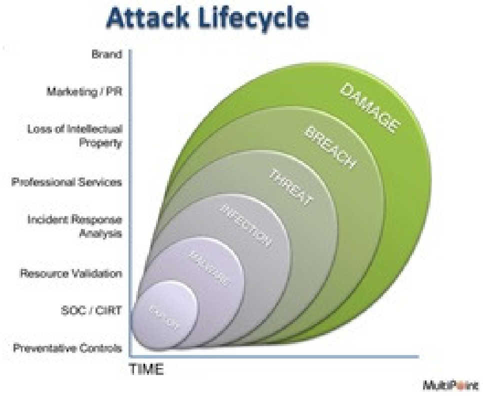

**Figure 2: Attack Lifecycle**

The Attack life cycle illustrates the periodical outcomes when the preventive control measures fails to mitigate the threat. It moves from initial exploit to damaging the brand or business besides the time moves on.

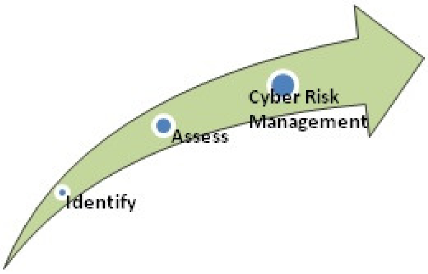

**Figure 3: Asset assessing stages**

The cyber security management will be done by initiated with identification, assessing then risk management by required calibration as shown in the picture.

3. **The NIST cyber security framework:** Thisalso insisting to assess the assets as the foremost thing in the cyber security framework.

- Identify
  - Asset Management
  - Business Environment
  - Governance
  - Risk Assessment
  - Risk Management Strategy
- Protest
  - Access Control
  - Awareness and Control
  - Data Security
  - Info Protection Process and Procedures
  - Maintenance
  - Proactive Technology
- Detect
  - Anomalies and Events
  - Security Continuous Monitoring
  - Detection Processes
- Respond
  - Response Planning
  - Communications
  - Analysis

  - Mitigation
  - Improvements
- Recover
  - Recovery Planning
  - Improvements
  - Commutations

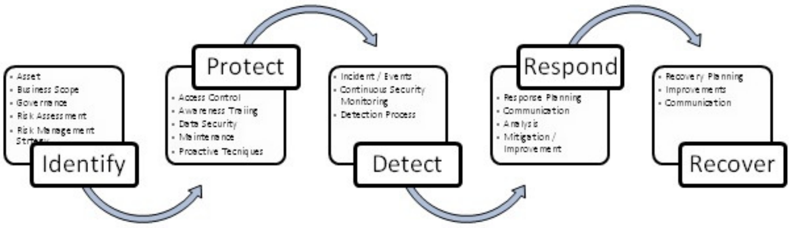

**Figure 4: Stages of NIST suggestions**

Over the past few years, India has massive adoption of cyber technologies in all the facets of life.

**4. Vulnerability Management Lifecycle:**

1. Policy : Establish Process, standards and guidelines
2. Inventory: Discover all assets across the network
3. Privatize: Assign Business value to assets
4. Vulnerability: Determine vulnerability on assets
5. Threats: View potential threats
6. Risk: Determine Risk Level = A x V x T
7. Remediation: Proactively fix vulnerabilities
8. Measure: Measure impact of security decisions and actions
9. Compliance : Review for policy compliance

Finally incorporating the automation for an effective vulnerability monitoring and mitigating the risk.

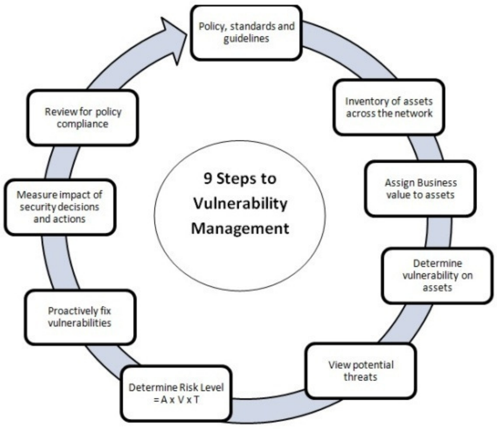
Policy, standards and guidelines
Inventory of assets across the network
Assign Business value to assets
Determine vulnerability on assets
View potential threats
Determine Risk Level = A x V x T
Proactively fix vulnerabilities
Measure impact of security decisions and actions
Review for policy compliance
9 Steps to Vulnerability Management

**Figure 5: Nine steps of vulnerability preventive mechanism**

**Step 1:** Identify the assets of the organization or business and decide the economical value of the asset to your business. Physical assets and virtual assets also must be identified like network, network devices, operating system, applications, servers, hosts, routers and other hardware and software things besides the virtual assets like people they are coming in to your through internet. Specifying the every assets name, version, location used and approximate rating in which it is helpful in your business process.

Prioritizing the assets is an important step. The devices such as

- Network-based
  - Known and unknown devices
  - Determine network based applications
- Agent-based devices
  - In-depth review of the applications and patch levels
  - Deployment disadvantages
- Network and agent based discovery techniques are optimal
  - Agents – cover what you know in great detail
  - Network- identify rogue or new devices
- Frequency
  - Continuous, daily or weekly
  - Depends on the asset

This would be really useful while measuring the threat level with respect to that asset.

**Step 2:** Vulnerability Identification would be the second step in this process. Here, knowing what vulnerability exiting for an asset and its criticality of that vulnerability is important in determining how best to secure that asset. The threats could be correlate and identify its priority of required attention, because, not all threat and vulnerability have equal priority. Primary goal is to rapidly protect the most critical assets. Threat identification includes finding of worms, exploits, wide-scale attacks or advanced persistent attacks and new vulnerabilities. All these could be correlate with the most critical assets, so that final result would be a good prioritization of vulnerability within the organization environment.

**Step 3:** Regular vulnerability management is most required to get high frequency scanning of the environment and to reduce the volume of vulnerability from any scan. The frequent scanning will find out any new vulnerability and the remedy could rectify before a great loss.

**Step 4:** Risk Assessment is another step here to calibrate for accurate and timely details on the vulnerability that exist. Risk assessment also should be done in a frequent manner to determine the risk level in time. Risk could be calibrated by the following formula by substituting vulnerabilities, assets and threats, Risk = Vulnerability x Asset x Threat.

Based on the criticality of each component of the risk formula, the risk value could be derived and it is easy for focusing on the risk.

**Step 5:** Integrate the change management with a frequent vulnerability management process. Grading the Software system and newly added hardware and applications also could be tested regularly. All these could prevent new vulnerabilities.

**Step 6:** An effective vulnerability could include regular software patching and for the perfect results, step5 and step 6 must be incorporated.

**Step 7:** Other mobile devices escape traditional vulnerability and compliance methods, so these devices also should be considered and monitor during scanning. Generally, these mobile devices also should integrate with the monitoring system.

**Step 8:** Mitigation process should have an alternate mechanism to undertake the mitigation process during the occurrence of risk. To reduce the time delay during the traditional mitigation methods, the organization must possess some effective alternative mechanism to overcome such incidents. Firewall rules, increasing law of monitoring or enforcing procedural rules will work in such situations until fixing or mitigating the risk. This process is known as remediation resolution of risks.

Some organizations, they depend only on remediation methods to overcome risks instead of having mitigation methods because of the over cost incurred than the loss due to the particular risk. In Pareto principle says 80/20 rule, here, 80% of risk can be eliminated by addressing 20% of the issues. Rightly addressing the assets and its threats in a right time is important in this rule. When should patch or when should mitigate also should be predicted in an appropriate way.

**Step 9:** The response for the incident is the final step, and it shows the systems strength to combat the breach. An effective incident response will be possible only by having strong security response in a proactive methods and procedural controls in place to fix the vulnerability.

All these steps could be managed and executed by people but humanly error could be avoided and periodical scanning also could be achieved by automate the whole process for an effective output. At the same time mechanizing the process will be efficient and irrespective of the size of the system. So the final key to successful vulnerability management could be automation. So that detecting and remediation any vulnerability in time.

## 5. Conclusion

The vulnerability management is the key function in the proactive measures of the cyber security process. By controlling or fixing the vulnerabilities on a system, the organization need not bother about the cyber risks. It is suggesting to have a good methodologies to combat the vulnerability combat mechanism. The National Institute of Standards and Technology (NIST) framework for improving critical infrastructure cybersecurity, National Critical Information Infrastructure Protection Centre (NCIIPC) framework for evaluating cyber security in critical information infrastructure and other proven frameworks also insisting in that direction.

## 6. Bibliography

[1] McCarthy, C., Harnett, K., & Carter, A. (2014, October). A summary of cyber security best practices. (Report No. DOT HS 812 075). Washington, DC: National Highway Traffic Safety Administration.

[2] NIST, Feb 1, 2014 version 1.0

[3] Cyber security research developments, A NASSCOM Initiative, DSCI, 2013

[4] National Critical Information Infrastructure Protection Centre (NCIIPC) framework, 2014

[5] Cyber security and risk management, NCSC, 2013

[6] The CIS critical security controls for effective cyber defense Version 6.0, October 2015

[7] National Cyber Security Framework Manual, NATO CCD COE Publication, 2012

[8] http://www.beyondsecurity.com/vulnerability-management.html