A Systematic Study of Asset Management using Hybrid Cyber Security Maturity Model

Sai Sireesha Veerapaneni, K.Raja Sekhar

Abstract— There are persistent cyber security attacks which leads unauthorized access to internal corporate networks and other critical confidential information. It is essential to build security solutions by adopting a Security Framework for any organization to find solutions for majority of vulnerabilities and flaws. The proposed work provides a platform to study methodical, controlled and repeatable approach to assess an organization's cyber security posture especially for asset management. The study helps organization's owners to assess their operational and information system's cybersecurity practices by querying a set of comprehensive questions about cyber security assets like Authentication, Authorization, Access controls, Database, Email security, Removable media, Backup &, Firewalls, Incident management etc. The proposed model improves the cyber security posture of the organization and escalate the chances of mitigating cyber security risks.

Keywords: Cyber security, Cyber security evaluation, cyberattacks, Cyber Security Assets, Maturity Assessment

I. INTRODUCTION

Cyber security can be defined in many ways. It can be considered as a set of techniques used for the security practice to defend computers, servers, mobile devices, electronic systems, networks, and data from several cyber-attacks. However, now it has been extended and included other aspects like infrastructure, information assets, people and processes [1]. Understanding about cybercrimes and cyber security is a must to reduce the cyber-attacks.

Achieving the security posture is a challenging task for many organizations. It is very important to maintain sustainable security environment because to protect the sensitive data of the customers and organization from the hackers. In today's world every organization can be affected by different kinds of cyber-attacks. It is always better to prevent the attack rather than responding to the attack after it occurs. Organization should adopt offensive and defensive measures to build a secure environment. These measures play a crucial role in developing an effective security posture in an organizational level. Each organisation possesses different domains and assets.

The work considers each security category in cyber security domain as a cyber-security asset. All existing maturity models were evaluated in domains with few limitations. For instance, security category (Authentication) is used in different domains and the maturity is calculated in a different manner as the authentication mechanism is adopted from different solutions, process and polices. In this proposed model we considered each security category as an asset and posed related questions to understand the existing process and controls. We also consider the recommendation controls to the respective cyber security asset.

Some of the cyber security assets in the organization are Authentication, Authorization, Sensitive data, Exception Management, Auditing and logging, Cryptography, Database, Access control, network, Configuration, error information disclosure, Data, Firewall configuration, security awareness training, secure development guidelines, Backup & restoration and many more …

Authentication: It is the process of validating and ensuring a user's identity. With complex authentication it is very hard for the hackers for breaking into the systems.

Authorization: The mechanism of providing security by specifying administrative and normal user privileges related to computer system security which includes files, programs, services and other features.

Sensitive Data: Data should be classified by data owner like public, internal, restricted, highly restricted and critical. Security controls should be implemented based on the data classification.

Exception Handling: It is used to protect error information to attackers/unauthorized users. Hackers would construct attacks based on disclosed technology information.

Auditing& Logging: It is a diagnostic method which is used to investigate after a security incident. Logs should be noted as read-only mode and not store any sensitive information.

Database Security: Database is the collection of data including stored function, database systems and servers. The data in database can be easily accessed, modified and manipulated. So security should be provided.

Access control: It is a process of granting access to the users and certain privileges to resources, systems and information. Credentials must be presented by users before granting the access.

Email-Security: Email is a popular security platform for spreading malware, spam and other attacks. So providing security for an email communication is essential in organizations.

Revised Version Manuscript Received on March 08, 2019.

Sai Sireesha Veerapaneni, M.Tech Student, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. (e-mail: vssirisha95@gmail.com)

Dr.K.Raja Sekhar, Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. (e-mail: rajasekhar_cse@kluniversity.in)

Most of the organizations allow Email application to be handled through Authentication procedure allocating access levels and creates a user hierarchy with policy. These policies will be put together and be part of the proposed framework.

Firewalls: A Firewall can be software or hardware or can be combination of both. Firewall is a network security system designed for the purpose of preventing unauthorized users entering into the private networks.

Incident management: It is the process takes place after an incident happened in an organization. It is the process involves steps like identify, analyze and taking steps to prevent the incident happening in the future. This is an important process which should take place in the right time.

Security awareness training: It is the process of educating employees in an organization about their procedures and corporate policies for developing a secure environment in information technology in an organization.

Secure guide lines should be developed and followed by all the IT and NON-IT employees in an organization.

Security Audit: It is the process of technical and manual assessment of a system or application and employees in an organization.

Backup & Restoration: It is the process used in case of data loss. Data backup process can be done only when copying and archiving data is done. So that data can be accessible in case of deletion and disruption. Restoration is important in case of any incidents happened in the organization level.

Removable media: This term referred as data storage devices which can be removed without powering off the system. This devices can transfer data easily from one system to another system. CDs, DVDs, USB drives, Bluray, disks are some examples of removable media.

This model gives asset based assessment. The term assessment means it collects and reviews the data in-order to improve the current performance of an organization. Assessing each asset in the organization leads to the improvement of security in all domains.

2. SYSTEMATIC STUDY OF EXISTING MATURITY MODELS

Maturity models are expertise by effective planning, managing, responding to threats and recovering from exposure. In the developing world, many organizations cannot provision themselves with needed technology, or able to integrate capabilities to achieve security posture within their organisation. Accomplishing different levels of maturity is one of the most essential method to state the organization cybersecurity readiness. This can be done by maintaining a set of requirements to aid in progressively. There are some maturity models existed for the efficient development of security posture in the organization. Some of the frameworks will be discussed in the subsequent content mentioned below

2.1 NIST Cyber Security Framework:

It is a framework which has been issued within critical infrastructure sectors in order to provide guidance for the organizations to moderate the risk associated with security. It is a framework but not a maturity model so there is a need of an existing maturity model or build a new one to measure the CSF implementation progress.

NIST CSF implements critical infrastructure to enhance the security postures of organizations. It is generally recommended for organizations to complement the existing cyber security maturity model in the organization. This will help to define their improvement areas.

2.2 The Cyber Security Capability Maturity Model (CM2)

CM2 is developed to attain and sustain security advantage by providing guidance on the necessary requirements. Society, technical, operational, business, legal and regulatory, and education/capability building measures are the principal underlying measures. CM2 can serve as the basis of comparative assessment across nations and enhances over time cross-border collaboration through buy-in [1].

A model is proposed to elevate security posture by improving the capabilities. The stages of CM2 in turn influenced by 5-factor model as the premise for capability development in cybersecurity. This model is proposed to attain defendable security advantage. All countries should dynamically build its capabilities to defend threats, vulnerabilities.

2.3 The Community Cyber Security Maturity Model (CCSMM)

This model was proposed to define healthier methods to outline the existing state of the communities in its cyber readiness and also to provide a roadmap for organizations to follow in their groundwork. This model includes different elements to address the issues faced by different communities. This model defines metrics, technology that is required and addressing threats, processes to communicate between the dissimilar community bodies, and tests which can be used along with the metrics to evaluate the current status of a community's security preparedness level. Community can actually possess organizations that are at different levels in the model at the same time. This model can differentiate between the different community organizations and their own level of cyber security readiness.

2.3.1 The five maturity levels are:

1. Security Aware: In this level the activities are carried out to make organizations and individuals aware of the threats, problems, and issues related to cyber security.

2. Process Development: In this level elements are designed to effectively address cybersecurity issues by establishing and improving upon the security process required.

3. Information Enabled: In this level specifies the awareness of all organizations within communities about security issues and having methods and mechanisms in right place which is used to assess security relevant events. The aim of the improve information sharing mechanisms among the organizations in the communities.

4. Tactics Development: IN this level more proactive methods are developed to efficiently address against threats and attacks .More prevention methods comes into place by this level.

5. Full Security Operational Capability: This is the top level of the model. In this level elements are developed to place the entities in the organization in a safe place so that prevents attacks and threats by doing everything they could.

2.4 A Security Engineering Capability Maturity Model

A SECMM is developed to improve the process in the practice of security engineering. It gives a framework for a mature security engineering process and organization that can lead to better, cheaper, and faster development of secure systems and products. It contains a sequence of levels that guides the security engineering organization towards process improvement through small steps. The goal is to develop an organizational culture of continuous process improvement. This model has five maturity levels. Those levels represents the maturity of security organizations.

2.5 Limitations of existing models:

• All models can be adapted to different types of organizations; however, they need some level of customization.

• All Models perform different types of processes to get the maturity of cyber security. But there are no other models that work on assets, system components and all services of organization to evaluate individual maturity level.

• The cybersecurity capability maturity models need a level of customization to implement in an organization.

• All cyber security capability maturity models are based on cyber security risk management not on the asset maturity.

3. PROPOSED MODEL

Figure 1. depicts the architecture of our proposed model named as Cyber Security Assessing Maturity for Organization (CSAMO). The model is built on IT firms for Category Based Maturity Evaluation. The Maturity Model has been divided into below modules.

- Cyber Security Asset Inventory
- Cyber security Asset Questionnaire
- Maturity Level Logic
- Asset Recommendation Solutions
- Reports/charts
- Database

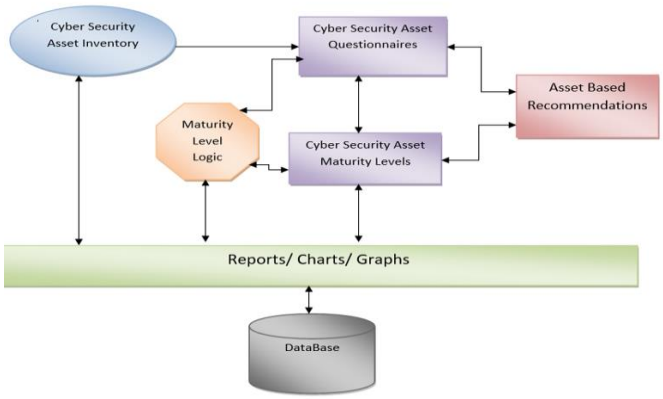

Figure 1: Architecture

3.1 Cyber Security Asset Inventory: It is a collection of all cyber security assets. Each and every asset has to be identified with the below details.

- Asset Name
- Asset Priority (High, Medium , Low)
- Asset type
- Asset Description
- Asset Starting Date
- Asset Expiry Date
- Asset Used Domain
- Asset Owner

Figure 2 gives a screen shot about Asset Inventory

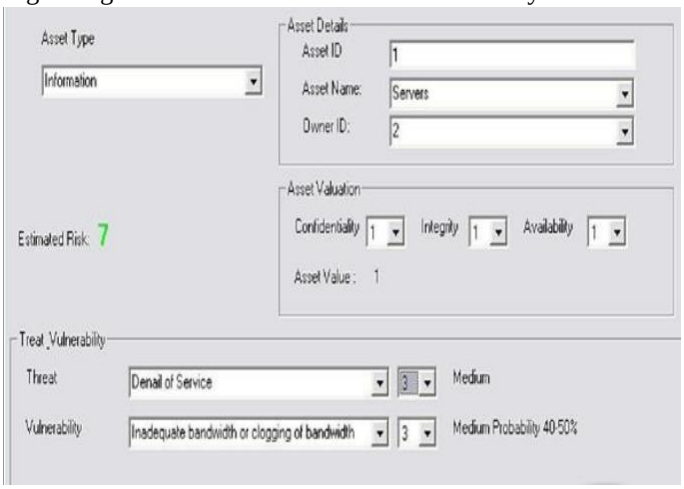

Figure 2: Asset Inventory

Asset can be added/modified/deleted from the cyber security asset inventory. There is an option to sort the asset based on priority, owner, and type. This inventory has a search option to find the existing asset from the list.

3.2 Asset Questionnaire: This module is having the comprehensive list of questions about the cyber security asset. Questionnaire covers the controls, practices and policies which supports all domains. Figure 3 depicts the specified module

Here we have given 4 options to each and every question to understand the existing practices for the asset. Options are as mentioned below

I. Not implemented
II. Partially Implemented
III. Fully Implemented
IV. Continues Improvement

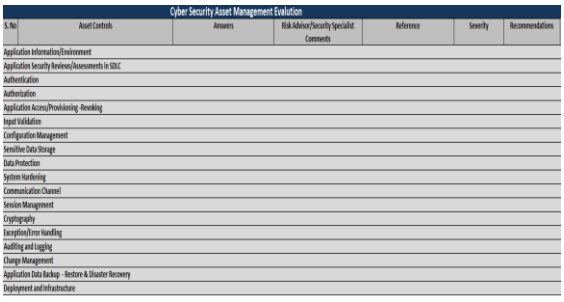

Figure 3: Asset Controls

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Question-driven approach helps to expose the highest-risk design considerations and the security frame helps you to focus on the areas that reveal common mistakes. The module is implemented in detail that gives the list of controls, questions related to Cyber Security Asset as shown in Figure 3.

3.3 Authentication:

- Is the Authentication mechanism planned/implemented for all domains? (Ex: form/windows/LDAP/SSO etc.⋯)
- Does authentication happen in SSO service?
- Are passwords required to immediately change the initial sign-in application?
- Does the system/device/application require passwords to change regularly?
- Is password entry for the system/device/application masked during sign-in?

And many more….

3.4 Authorization:

- Do all applications integrate with any access manager product? (Oracle access manager, Tivoli access manager, CA access manager etc⋯)
- Does the system/device/application accounts have least privilege?
- Is there any existing process to request access to the system/device/application?
- Is there any existing process to revoke access to the system/device/application?
- Does the system/device/application maintain user access control list?

And many more…

3.5 Sensitive Data:

- Is sensitive data classified in the organization?
- Does the sensitive information secured at storage?
- Does access control implemented to sensitive files?
- Have you protected the sensitive information at transmit?
- Are users/application/system passwords encrypted at storage? (Y/N)

And many more …

3.6 Exception Management:

- Does application design outline a standardized approach to structured error/exception handling the application?
- Does application exception handling minimize the information disclosure in case of an error / exception?
- Does the application store errors/exception in the error log?
- Does the application display generic/customised error message?
- Does the application use platform specific error handle libraries?

And many more …

3.7 Auditing and Logging:

- Does the design identify the auditing level, logging necessary and key parameters to be logged and audited?
- Are the user and system actions logged sufficiently for audit purpose?
- Does the application architecture identify the storage, security, and analysis of the log files?
- Are log files and application source files stored in the same location? (Y/N)

And many more …

3.8 Maturity Level Logic: This module contains the business logic to calculate the maturity of each cyber security asset and organization's cyber security maturity. When the user selects the cyber security asset questions, each answer to the question carries specific score based on the option provided by the users. Figure 4 lists the criteria for evaluating the said parameters

Cyber Security Asset Managemnt Evaluation

		Maturity		
Cyber Security Assets	Current	1	2	3
Authentication	0.00	0.00	0.00	0.00
Authorization	0.00	0.00	0.00	0.00
Sensitive Data	0.00	0.00	0.00	0.00
Exception Handling	0.00	0.00	0.00	0.00
Auditing and logging	0.00	0.00	0.00	0.00
Database security	0.00	0.00	0.00	0.00
Design Analysis	0.00	0.00	0.00	0.00
Access Control	0.00	0.00	0.00	0.00
Security Testing	0.00	0.00	0.00	0.00
Email security	0.00	0.00	0.00	0.00
Firewall	0.00	0.00	0.00	0.00
Incident Management	0.00	0.00	0.00	0.00

Figure 4: Cyber security Asset Management Evaluation

Once calculate the scores of all questions related to specific cyber security asset to analyze the maturity of the specific asset. It also provides specific recommendation solutions to improve the maturity of this cyber security asset.

After user answered to all cyber security asset questions, the scores are calculated based on the answers and provides the report of final maturity level of organization. The exact recommendations to improve the exiting maturity of organization also provided.

3.9 Recommendation Solutions: It contains comprehensive list of the recommendation controls of the cyber security asset. When the user selects the options, this tool will display the recommendation controls.

User needs to select the existing recommendation controls from the available list to calculate the exact score of that particular question.

See the below few recommendation controls of cyber security asset.

Authentication:

- Using of strong passwords.
- Support password expiration periods and account disablement.

- Never store credentials.
- Protecting authentication tokens by encrypting communication channels.

And many more …

Authorization:

- Use less-privileged accounts.
- Authorization granularity can be considered.
- Enforcement of privileges separation is to be done.
- Restrict user access to system-level resources.

And many more …

Sensitive Data:

- Avoid storing confidential data as plain text.
- Encrypt confidential data over the wire.
- Communication channel is to be secured.
- Provide strong access controls for sensitive data stores.

And many more …

Exception Management:

- Use structured exception handling.
- Do not reveal sensitive application implementation details.
- Logging of private data such as passwords should not be done.
- A centralized exception-management framework is to be considered.

And many more ….

Auditing and Logging:

- Malicious behaviour identification.
- Monitor good traffic and analyse how it looks like.
- Audit and log activity through all of the application tiers.
- Secure access to log files.
- Back up and regularly analyse log files.

And many more …

4. RESULT & REPORT

These modules collate all the information provided by users against the cyber security asset and generate the reports. Reports can be downloaded into different types

- Html based report
- PDF based report
- Doc based report
- Xls based report

Figure 5: Asset risk statistics

These reports gives the complete information of assets involved in criticality, scope and its maturity level, recommendations. The above Figure 5 depicts the same through pie chart

The below kind of graphs will be generated

- Top 10 strong assets
- Top 10 weak assets
- All critical assets
- All high assets
- All medium assets

5. WHO CAN USE THIS METHODOLOGY

A methodology for assessing cyber security maturity for an organization was defined with flexibility such that it would be utilized by small, medium, and large organizations (Government, Private and Educational) using any style of development.

As our model is completely based on cyber security assets, it will be useful to organization teams to improve their cyber security control to their own assets.

Business Owners: Individuals performing decision making activities on business requirements.

CISO: Head of Cyber Security in the Organization, Asset owner, data owner, Organization board members.

Managers: Individuals performing day-to-day management of development staff.

Security Experts: Individuals performing cyber security activates in Organization.

Developers: Individuals who write code to develop the software.

Support Operations: Individuals performing customer support or direct technical operations support.

Clients: Individuals who can work/adopt the services of software in the organization.

6. ACKNOWLEDGEMENT

This work is supported by the eSF Labs Ltd as part of the project/consultancy work taken by Department of Computer Science and Engineering of KLEF. I am very thankful to all my colleagues at eSF Labs Ltd. for their continuous support and helping me in completing the project.

7. CONCLUSION

It is a complete cyber security asset based model where these assets can be used anywhere in the cyber security area without reassessment. It is flexible, adoptable, reusable, time and process benefits, easily maintainable and cost saving approach compared to other models. This model is adaptable to small, medium and high level organization. It gives the accurate cyber security maturity assessment for the organization. Centralized cyber security assets which can be used in existing and new domains without re-maturity assessment. This will reduce the process, people and time while creating new domains.

This model gives a better understanding of the organization's cybersecurity posture; to improve cyber practices and maturity model of organization where there is a need for effective cybersecurity practices, identification of cybersecurity improvement areas and other solutions/Recommendations.

It avoids the duplication of controls which are used in different domains. Recertification Revalidation on existing cyber security assets is very easy because there is no need to test entire domain.

8. REFERENCES

1. Corlane Barclay "SUSTAINABLE SECURITY ADVANTAGE IN A CHANGING ENVIRONMENT: THE CYBERSECURITY CAPABILITY MATURITY MODEL (CM2) "IEEE 6858466.

2. Gregory B. White "The

Community Cyber Security Maturity Model" IEEE 4076571.
3. Online "Assessment" icss-cert.
4. Online "Resources available for those impacted by Roosevelt Fire" wyohomelandsecurity.
5. Sultan Almuhammadi, Majeed Alsaleh "INFORMATION SECURITY MATURITY MODEL FOR NIST CYBER SECURITY FRAMEWORK" aircci vol7, csit76505.
6. Richard M. Adler "A dynamic capability maturity model for improving cyber security" IEEEXplore 10.1109/THS.2013.6699005
7. Corlane Barclay "Sustainable security advantage in a changing environment: The Cybersecurity Capability Maturity Model (CM2)" IEEEXplore 10.1109/Kaleidoscope.2014.6858466
8. "Cybersecurity Assessment Tool " FFIEC May 2017
9. Nancy R. Mead ; Dan Shoemaker "The software assurance competency model: A roadmap to enhance individual professional capability" IEEEXplore 10.1109/CSEET.2013.6595243
10. Ganesh B. Regulwar ; V.S. Gulhane ; P. M. Jawandhiya "A Security Engineering Capability Maturity Model" IEEEXplore 10.1109/ICEIT.2010.5607700
11. "Software Assurance Maturity Model 1.0" Open samm
12. Ngoc T. Le , Doan B. Hoang "Can maturity models support cyber security?" IEEEXplore 10.1109/PCCC.2016.7820663
13. Richard Nilsen "A Developmental Study on Assessing the Cybersecurity Competency of Organizational Information System Users" Digital Commons Kennesaw State University
14. "Usable cyber security competency framework" Deliverable 3.2 ECESM