Ferdowsi University of Mashhad

Journal of Computer and Knowledge Engineering

https://cke.um.ac.ir

انجمن فناوری اطلاعات و ارتباطات ایران

Information and Communication Technology Association of Iran

A Model to Measure Effectiveness in Cyber Security Situational Awareness*

Research Article

Motahareh Dehghan[1], AmirAbbas Mahdi Zadeh[2], Babak Sadeghiyan[3]

DOI: 10.22067/cke.2024.83723.1101

Abstract: Cyber security situational awareness is a rather new concept in cyber security, which refers to an understanding of the cyber threat within an environment and its associated risk and impacts by the cyber security officers. This paper provides a model to measure whether security events, such as the occurrence of an attack or the selection of countermeasures, have been effective in the success of organizational missions. Two components are considered as inputs for this purpose. One is the Network Dependency Graph, which demonstrates how different assets in the network are dependent on each other and with what intensity or weight they affect each other. Another is the Mission Dependency Graph, which specifies the relation between organizational assets, tasks, functions, and mission objectives. It also specifies the impact of the assets on the organizational tasks, functions, and mission objectives. This paper aims to assess the impact of attacks on different assets with consideration of the organizational mission. The model's expression is in such a way that it helps different organizations with specific goals and requirements to use this model, and they can personalize and customize its different components. This model can be employed for critical asset recognition. Moreover, it enables us to know which countermeasures are more effective regarding the organizational mission. In this way, a quantitative and reliable statement will be employed between the security specialists and the non-expert beneficiaries of an organization.

Keywords: Measure of Effectiveness, cyberattacks, situational awareness, impact assessment, mission, mission dependency graph, network dependency graph.

1. Introduction

Despite the high importance of cyber security, many organizations still do not have a proper understanding of it and how to protect their assets against cyberattacks properly. This can lead to significant damages and potentially devastating consequences for a business.

This lack of understanding is mainly due to the misconception that cybersecurity is only the responsibility of the IT department. Although information technology significantly contributes to protecting an organization's network and data, cybersecurity is the responsibility of all employees and managers of the organization. Every employee is effective in protecting the organization's assets, whether through correct password management or consciousness against phishing attacks.

According to Endsley [1], "situational awareness is the perception of environmental elements in a time and space, comprehension of their meaning and projection of their status in the near future."

Organizations may employ security tools such as Intrusion Detection and Prevention Systems (IDS/ IPS) and Security Information and Event Management (SIEM) for perception of environmental elements to improve their cyber security situational awareness. These tools can monitor an organization's network in real-time and identify possible threats, such as unauthorized access or malicious activities.

A measure of effectiveness helps us to assess the effectiveness of cybersecurity efforts and the impacts of attacks. It is employed to determine how much the cybersecurity efforts or attacks improve or deteriorate the organization's cybersecurity situation.

By combining an organization's cyber security mission and measure of effectiveness, organizations can identify their critical assets and ensure that these assets are properly protected. For example, if an organization's mission is to provide online financial services, the organization's financial data must be protected, and its confidentiality must be ensured. Organizations can ensure that their cybersecurity efforts are adjusted with their mission to identify and protect their critical assets. This assures organizations that their cybersecurity investments are not being wasted on protecting assets that are not essential to their mission.

This paper is conducted to provide a model to measure the effectiveness of the organization's cybersecurity efforts, that is, to determine whether security events such as the occurrence of an attack or the selection of countermeasures have been effective in the success of the organizational

* Manuscript received: 2023 August 1, Revised, 2023 November 1, Accepted, 2024 March 10.

[1] Corresponding Author, Assistant Professor in Department of Industrial and Systems Engineering, Tarbiat Modares University
Email: m_dehghan@modares.ac.ir.

[2] Master Graduate, Department of Computer Engineering, Amirkabir University of Technology.

[3] Associate Professor, Department of Computer Engineering, Amirkabir University of Technology.

mission. Two components are considered as inputs for this purpose. The first one is the network dependency graph, which demonstrates how different assets in the network are dependent on each other and with what intensity or weight they affect each other. Another component is the mission dependency graph, which specifies the relation between organizational assets, tasks, functions, and mission objectives. It also specifies the impact of the assets on the organizational tasks, functions, and mission objectives.

In the next section, we review the previous research, which was focused on the impact assessment of cybersecurity events without considering the organization's mission. Then, we state the problem and our proposed model in more detail. Finally, the conclusion is presented.

2. Literature Review

Previous research on the impact assessment of cyber security events has addressed different issues. Some researchers assess the impacts of attacks on various assets. Some calculate the impacts of attacks on security objectives based on a mission sense, and others examine how effective situational awareness systems are.

One of the metrics in [2] applies the attack graph to identify vulnerabilities and assess the chain of actions performed by a malicious adversary to assess the impact of attacks and vulnerabilities on each other. That metric attempts to assess security and select countermeasures by employing an attack graph. Moreover, it prioritizes different paths of attack graphs by using probabilities, risks, and CVSS metrics.

In [3], another metric is proposed to obtain a numerical model to assess the current situation and predict the future situation of cybersecurity. This model aims to express the security of various network assets numerically, present their impact on the network, and calculate the probability of using threats to attack the system at a certain time using the Markov chain.

In [4, 5], a model for combining CVSS metrics using a Bayesian network is proposed. In those papers, the CVSS score is first converted into probabilities, and those probabilities are then propagated in different paths of an attack graph to obtain an overall metric. That metric pays special attention to loops in the attack graph. It allocates the probabilities using a Bayesian network, and the overall metric is then obtained through the Bayesian network. Finally, it is suggested to use dynamic Bayesian networks so that the changes in networks and vulnerabilities can be considered over time. That metric calculates the probability of exploiting a vulnerability.

Chung et al. [6] introduce a model to choose countermeasures according to the characteristics of cloud systems. They try to identify the virtual machines that have turned into zombies by developing an attack graph and using the intrusion detection core to choose a security measure from the existing pool of security measures regardless of the organization's mission to eliminate the threat. The core of this model is attack analysis, such as developing an attack graph, combining threat notifications, and choosing countermeasures in the cloud.

In [7], the number of vulnerabilities needed to penetrate the network is calculated instead of ranking unknown attacks. The higher the number of vulnerabilities, the lower the probability of exploitation, indicating greater security because the probability of availability of unknown vulnerabilities is much lower.

As stated before, some researchers propose solutions for impact assessment by considering the organization's mission. In [8], the impact of the current attacks is calculated, and the possible impacts of the current attacks in the future are estimated by employing the impact assessment graph, which is generated by combining the attack graph and network dependency graph. That graphical model practically eliminates the semantic distance between known vulnerabilities, missions, or services that can be affected. Impact assessment graphs can be used to follow the progress of the attack, monitor the network status, and assess the damage at the same time. The network status should be updated whenever a successful exploit is detected. However, only the status of directly or indirectly affected components should be updated according to the structure of the dependency graph.

The impact on the mission can be defined as a conditional probability according to the mission dependency graph, the network graph, and a set of external events. Obtaining the value of this probability is known as the problem of mission impact assessment [9].

Kheir et al. [10] propose a new service dependency representation that enables intrusion and response impact evaluation. The outcome is a service dependency model and a complete methodology to use that model in order to evaluate intrusion and response costs. The latter covers response collateral damages and positive response effects as they reduce intrusion costs.

Different situational awareness systems can be used in an organization to measure different metrics. The situational awareness system should be assessed as well. Some metrics are provided for this purpose [11]. These include metrics such as credibility, purity, and cost-effectiveness.

There are studies on the detection of dependencies between assets used in tools such as Paris [12], AID [13], and CloudScout [14].

FarahaniNia et al. [15] proposed a system to assess the impacts of attacks on cyber assets and identify critical assets. In their proposed system, the business process model of an organization and the dependency between the process and cyber assets should be generated. Then, the system simulates the attacks on cyber assets and evaluates the impacts of attacks on the cyber assets and processes.

From another point of view, the relationship between risk assessment and MoE can be expressed.

The methodology of the information security risk management, containing risk identification, risk analysis, risk evaluation, and risk treatment, uses the frameworks of ISO 27005, ISO 27002, ISO 27011, OCTAVE, and NIST 800-30 and OWASP standards [16].

In [16], a method for managing risks within an IT department of a telecommunication company in Iran was proposed. That method identifies the risks that require immediate attention and those that can be tolerated within the company's risk management framework.

In [17], a framework is designed to evaluate the security status of a network from three distinct dimensions: the assessment of threats, analysis of vulnerabilities, and evaluation of stability. These dimensions are then integrated at the decision-making level to gauge the overall security situation of the network.

This paper proposes a model to measure the effectiveness of cyber security events by considering the organization's mission. The proposed model can be used and personalized by different organizations in a scalable and timely manner. In the next section, we state the proposed model in more detail.

3. The Problem Statement and The Proposed Model

To implement a cybersecurity situational awareness system in an organization, a knowledge stack covering network infrastructure, cyber posture, cyber threats, and organization mission dependencies is required. Then, a model to assess the impact of various cyber security events on organizational mission is essential. This model can determine the impacts of attack and countermeasures on organizational missions.

In this regard, some issues should be addressed, including the organization's various assets. Moreover, one should know what is the relationship between different assets and to what extent they affect each other.

Furthermore, the graph of the organizational mission should be generated; that is, the relationship between the assets, tasks, functions, and mission objectives is determined.

The proposed model for this problem has two basic requirements. First, the network dependencies must be determined, which means what assets are in the organization's network and what is the relationship between them that may not even be evident at first. It should also be noted that the assets may be in the cloud computing platform, and the relevant assets may be added or removed during the life cycle of the system.

The next requirement is to know how these assets affect each other and, ultimately, the organizational mission, that is, to know how much the organizational mission is dependent on each of the assets.

3.1. The Proposed Model

In this section, a model is proposed to measure the effectiveness of cyber security events and to know how much the security objectives stated in the organizational mission have been achieved. In this regard, the parameter E_m or Mission Efficiency is defined, indicating how many percent of the mission has been completed at the moment.

E_m is supposed to be obtained based on the effectiveness of assets, indicated by E_s; that is, mission effectiveness is achieved through the effectiveness of each organization's assets, as stated in Equation (2). For example, if there is only one asset, the mission effectiveness depends only on this asset. If this asset is lost and its effectiveness becomes zero, its mission effectiveness becomes zero, too. Table 1 illustrates the defined parameters which are used in equations.

There are some models which are appropriate for this condition. One of these methods is AHP/ANP, through which the weights can be calculated in a hierarchy [18, 19], or these weights can be obtained through questionnaires.

A suggested hierarchy is to break each mission into some tasks, with each task containing some assets. The security effectiveness of each asset is divided into different security dimensions of confidentiality, integrity, and availability, which are also called the acronym CIA. Each dimension of the CIA for each asset can be defined through some functions. For example, the error rate of a web service can be used to define the availability of an asset.

Table 1. Defined Parameters

E_m	Mission effectiveness
E_{ti}	Task i effectiveness
E_{si}	Service i effectiveness
W_{ti}	The percent of the impact of Eti in Em
W_{si}	The percent of the impact of Esi in Eti
N	Total number of tasks
N_i	Total number of services related to task i
F, G	Some function

For more clarity, assume an organizational mission as providing a messenger service. It is supposed to determine the impacts of various events on mission effectiveness. These events include attacks, any action caused by human error, changes in the network design, or selection of countermeasures. The primary option would be referring to the experts' opinions. However, descriptive methods that do not have an accurate basis will not be sufficient in general. A method is required to measure the mission's effectiveness. Here, a tree is generated whose root is the mission, the leaves are the running services, and the edges are the relationships between the services and the mission, as illustrated in Figure 1. A service may affect the mission more than other services. Equation (1) and (2) gives the relation between mission effectiveness and asset effectiveness with different weights.

In the example mentioned above (an organization that provides messenger service), the failure of the user interface will have less impact on the mission than the message transfer service. Hence, the weight of the user interface would be less than the message transfer service.

$$\sum_{i=0}^{N}(W_{s_i}) = 1 \qquad (1)$$

$$E_m = \sum_{i=0}^{N}(E_{si} \, . \, W_{si}) \qquad (2)$$

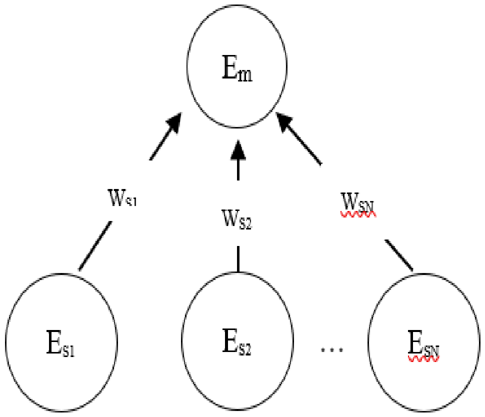

Figure 1. The first proposed tree for a measure of effectiveness

The question is how to obtain the weights. To respond to this question, it should be noted that these weights are obtained based on the application of services by considering the mission. There will be various dependencies between the services due to the way of choosing and employing the services. So, these weights depend not only on the service but also on the mission and the way the organization uses the services. Accordingly, these weights should reflect the meaning of the service in satisfying the mission. Since humans define the mission, these weights must be defined by humans. However, the difference of opinions should be minimized.

One solution is to hold a meeting consisting of security experts and other technical and even commercial experts of the organization, and their consensus on those weights can be obtained. Another solution is to think of other methods, as the previous method is not very accurate. For example, other multi-criteria decision-making methods can be considered. So, a more accurate model for finding the weights would be favorable. In the previous model, each expert must make N$_i$ comparisons to express their opinion.

AHP is one of the models that can be used. In this model, the number of comparisons is reduced to $\frac{n \times (n-1)}{2}$.

To reduce the number of comparisons, services that are completely dependent on each other are divided based on a new task order. This reduces the pairwise comparisons to be reduced more. Equation (3) describes the relation between mission effectiveness, task effectiveness, and their weights. At the same time, Equation (4) states the relation between task effectiveness, asset/ service effectiveness, and their weights. By combining these equations, mission effectiveness is obtained based on asset/ service effectiveness and their relevant weights. Figure 2 demonstrates the relationship between mission, task, and asset/ service effectiveness.

$$E_m = \sum_{i=0}^{N}((\sum_{j=0}^{N_i}(E_{sj} \,.\, W_{sj})).\, W_{ti}) \tag{3}$$

$$E_{ti} = \sum_{j=0}^{N_i}(E_{sj} \,.\, W_{sj}) \tag{4}$$

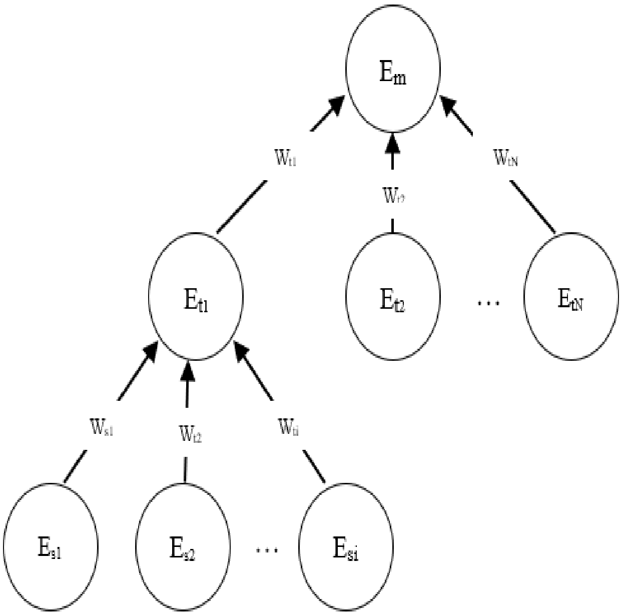

Figure 2. The second proposed tree for a measure of effectiveness

$$E_m = F\ (E_{t1}, E_{t2}\ldots, E_{tN}) \tag{5}$$

$$E_{ti} = G\ (E_{s1}, E_{s2}\ldots, E_{sN}) \tag{6}$$

However, there should be more elaboration on the calculation of E$_{si}$. In addition to the use of summation and multiplication functions to calculate the effectiveness of a unit based on its effective components, other functions may be used to indicate the dependence and impacts in the hierarchy, which we will discuss here. Equation (5) and (6) exhibits the general functions F and G. Some of the proposed operators might be weighted sum, multiplication, maximum, and minimum, which are described in the following:

Weighted sum

$$E_m = \sum_{i=0}^{N}((\sum_{j=0}^{N_i}(E_{sj} \,.\, W_{sj})).\, W_{ti}) \tag{7}$$

$$E_{ti} = \sum_{j=0}^{N_i}(E_{sj} \,.\, W_{sj}) \tag{8}$$

Multiplication (Exponent)

$$E_m = F(E_{t1}, E_{t2}, \ldots, E_{tN}\ ) = (E_{t1}^{Wt1}).(E_{t2}^{Wt2}) \ldots (E_{tN}^{WtN})$$
(9)

$$E_{ti} = G(E_{s1}, E_{s2}, \ldots, E_{sNi}\ ) =$$

$$(E_{s1}^{Ws1}).(E_{s2}^{Ws2}) \ldots (E_{sN}^{WsNi}) \tag{10}$$

Maximum

$$\begin{aligned} E_m &= F(E_{t1}, E_{t2}, \ldots, E_{tN}\ ) \\ &= Max(E_{t1}, E_{t2}, \ldots, E_{tN}) \end{aligned} \tag{11}$$

$$E_{ti} = G(E_{s1}, E_{s2}, \dots, E_{sNi}) = Max(E_{s1}, E_{s2}, \dots, E_{sNi}) \quad (12)$$

Minimum

$$E_m = F(E_{t1}, E_{t2}, \dots, E_{tN}) = Min(E_{t1}, E_{t2}, \dots, E_{tN}) \quad (13)$$

$$E_{ti} = G(E_{s1}, E_{s2}, \dots, E_{sNi}) = Min(E_{s1}, E_{s2}, \dots, E_{sNi}) \quad (14)$$

In the following, some of the design patterns [20] and the functions that can model them are examined. These design patterns represent some dependencies that can be formed between different services.

- ***Sidecar and Adapters: Identical Function***

Sidecar is a separate process that runs next to the primary service, providing additional functions. This pattern provides the possibility of separating concerns such as service discovery, load balancing, and security from the original service. This makes it easier to update the system without affecting the original service.

- ***Adapters***

Adapters are used to extend the functionality of a service by adding new features or modifying existing ones. Adapters can be used to integrate with different systems, such as databases or message queues, or to add new features, such as logging or monitoring. This pattern provides the possibility of developing a flexible and modular system that can be easily adapted to changing needs.

- ***Replication: The sum, multiplication, or maximum***

Replication includes keeping multiple copies of service or data in multiple nodes in a distributed system. This can be done by creating a copy of the service or partitioning data and distributing them in several nodes.

- ***Sharded: The sum, multiplication, or minimum***

Each shard in a sharded system is a separate instance of the database that stores a subset of data. The data are partitioned according to a shard key, which is a value used to determine which shard a piece of data belongs to. The shard key is usually selected based on the nature of the data and the expected system workload.

Several different methods have been proposed to implement partitioning, such as range-based partitioning, in which the data are partitioned based on a range of values, and hash-based partitioning, in which the data are partitioned based on the hash of the shard key.

- ***Scatter/Gather: The sum or multiplication***

The Scatter/Gather pattern can be used in various scenarios, such as distributed data processing, where a large dataset needs to be processed in parallel on multiple machines, or distributed search, where a single search term is sent to match multiple instances of a search.

- ***Queue: The sum***

As common approaches, queue design patterns are used in distributed systems to manage asynchronous communication and send messages to different parts of the system. In these patterns, messages or tasks are placed in a queue and then processed by one or more worker instances. This enables the separation of the message sender and receiver and allows the system to handle high-volume traffic and message processing.

- ***Batch processing: The sum***

As a design pattern, batch processing is usually used in distributed systems to manage large amounts of data and perform long-term tasks in a more efficient and scalable way. In this pattern, the data are processed in batches instead of in real-time. This enables the system to handle high-volume traffic and data processing.

3.1.1. Calculating E_{si}

E_{si} indicates the effectiveness of service i. E_{si} will be one if service i is fully provided and 0 if it is completely shut down or unavailable. This number can vary between 0 and 1 based on different events that may occur.

E_{si} is defined by the event. So, the services that measure various network events are queried to calculate E_{si}. For example, the SIEM service or Prometheus that keeps the status of various metrics over time is queried, and the outputs are converted into numerical values based on their meaning in a series of functions. For example, the E_{si} of an Nginx web service can be defined in such a way that the latency metric and status code are received from Prometheus every minute. The status will be healthy, and E_{si} will show the value of 1 if the status code is in the 2XX range, which indicates a healthy status in the HTTP protocol and the latency is below 20ms. If this web service responds with a longer delay or if the response status is not in the 2XX range, this metric will be less than 1. For example, E_{si} will be 0.8 if 20% of the requests return 403.

Some ideas for measuring confidentiality, integrity, and availability are provided below as examples.

For example, a suggested metric for confidentiality is the ratio of undisclosed data to all confidential data according to its importance.

Integrity is the ratio of correct data multiplied by the importance of correct data to all data.

Availability is the ratio of successful requests (in terms of error rate and response time) to all requests.

These cases are mentioned as examples, and different types of metrics may be used in the input layer of the model based on the organization's needs.

Moreover, methods such as the number of record lines, the volume of files, etc., may be used to measure the amount of data. The sensitivity of each data is the importance of different parts that are obtained during the weight allocation process. Data should be considered at the level of abstraction of a machine because smaller granularity over the data causes unhelpful complexity of the problem.

Another important question is what happens to the dependencies between services. Consider a simple example that the web service is dependent on the database service and that a problem occurs for the database. So, the web service that receives its information from the database encounters problems, and the web service metrics start showing these problems. For example, the web service may start giving a status code of 500, send requests with a delay, or show a query on the SIEM. This interruption can be seen in the web service logs. If there is no impact on the defined metrics, either the dependencies do not exist, or they have been covered through existing redundancies (for example, database backup service).

4. Evaluation

To evaluate the proposed model, a scenario is provided in this section. In this scenario, an organization that has the mission of providing event monitoring services to different organizations is examined. The tasks of this organization can be divided into user management, log management products, distributed tracking products, and so on.

Items such as user management database, user management web service, management web services, logs database, rejection database, etc., are considered as the assets of this organization. The attack scenario is assumed to be that the log management database and the rejection product database have been compromised and are out of reach. It must be decided which asset should be prioritized due to the limited resources. It is possible to determine how much the attack has affected the organization's mission effectiveness with this model. It can be checked how much of the lost effectiveness will be returned if any of these lost services return to the circuit, and the priority can be determined accordingly. Figure 3. provides a modified mission dependency tree for the above scenario. As it is seen in Figure 3, two paths transmit the negative impact from asset to mission.

In the following, the output of this model will be compared with the previous models and solutions through some examples.

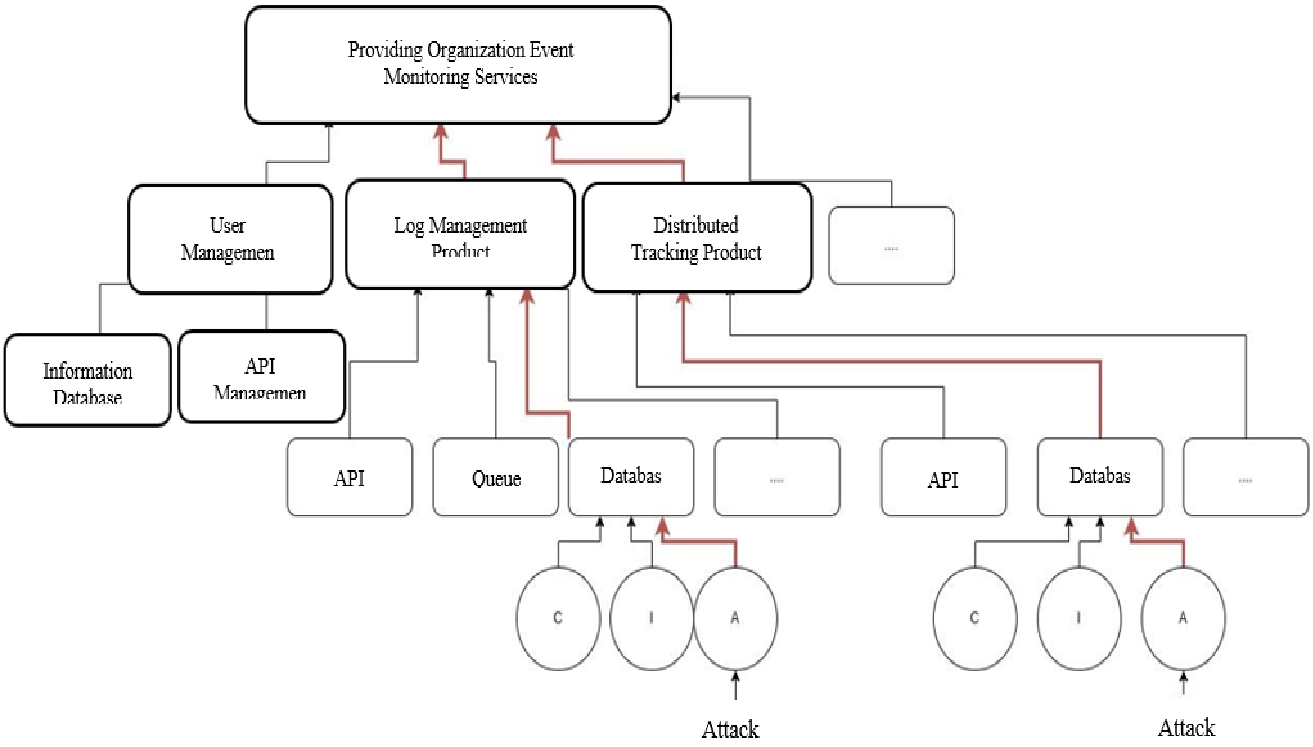

Figure 3. Example Scenario- Monitoring service provision system

Table 2. A comparison of the proposed model with the previous research

Paper	Proposed method, model, metrics, and system for impact assessment	Difference with our proposed model
Malowidzki et al. [2], Aissa et al. [3], Frigault and Wang [4], Khosravi-Farmad and Ghaemi-Bafghi [5], Chung et al. [6], Wang et al. [7]	New network security metrics were proposed.	The metrics of this group are used as input for our proposed model in the services and assets layers.
Albanese and Jajodia [8], Motzek and Moller [9], Kheir, et al. [10]	Methods that use organizational missions for impact assessment were proposed.	Our proposed model uses organizational missions, too. However, those proposed models are not comprehensive. They did not consider weighted relationships between different layers, different types of relationships between them, and design patterns.
Tadda and Salerno [11]	Some metrics for the assessment of situational awareness systems were proposed.	The models of this group can be used if our proposed model is relevant to the assessment of situational awareness systems.
FarahaniNia et al. [15]	A system to assess the impacts of attacks on cyber assets and identify critical assets was designed.	The measure of effectiveness used in [15] is as Equation (2) .It ignores the variety of relations between different layers and the design patterns.
Shirazi and Kazemi [16]	A method for risk management was suggested. That method identifies the critical risks that require immediate attention.	Our model delves into utilizing a more intricate methodology, such as the Analytic Network Process (ANP), to calculate the weight of the risks. It provides a quantitative model that demonstrates the effectiveness of changes in various aspects, thus facilitating a more comprehensive understanding of the risk management process and its efficacy.
Rongrong et al. [17]	A framework designed to assess the security situation of a network from three distinct dimensions: the assessment of threats, analysis of vulnerabilities, and evaluation of stability.	Our model attempts to assess the security situation from more dimensions: organizational mission, mission objectives, tasks, assets, threats, and vulnerabilities. Hence, our proposed model is more comprehensive.

4.1. Example 1

Assume that we have some files whose integrity should not be changed. For this purpose, some rules are defined on those files by employing Wazuh for notifying the modifications. These specified rules are then given as input to the model, and any possible changes are entered into the model in real time.

It is assumed that the integrity of a file is reduced from 100% to 50%. As the model receives this modification, it applies it to the mission dependency graph, and the final impact on the organization's mission is calculated based on the weights.

In contrast, the previous research [8-10], [17] generally determines the impact of the attack on other vertices of the network in the attack graph. As such, they are not done in real-time. In other words, they may show the situation of the network as being terrible, but a risky event may not have happened based on our mission. Conversely, an asset may be at risk, but it may not take into account how important that asset is.

4.2. Example 2

It is assumed that there is an organization that provides messenger services, consisting of three sub-services: message management, bot management, and group management. Assume that there is a vulnerability in the message management service, and the messenger service will be completely disrupted if that vulnerability is exploited. Previous research [16] can only determine that this risk exists and does not discuss the moment of exploitation. Second, they may argue that one-third of the effectiveness is reduced as there had been three sub-services, while one is lost. This does not match the real conditions because the meaning of different services is not the same, and each one has different effectiveness in real conditions. In these conditions, our proposed metric may state that you have lost five-sixth of your mission effectiveness, which might be closer to reality, as the message management service is more important than the other two services.

Table 2. presents a comparison of our proposed model with the previous research.

4.3. Discussion

To compare our presented model with the previous ones, it should be investigated what question the different models try to answer. The question raised by models such as the Markov chain [3], Bayesian networks [4, 5], etc. is how to investigate the impact of vulnerabilities on other network assets. This question determines a level of situational awareness that can be easily and even automatically calculated. However, is that level of knowledge sufficient? We don't think so. It should be checked how severe the attack affected the mission, even if it affected a large number of assets. A model more complex than a simple model that only considers the attack graph of network dependencies should be employed to answer this question.

The mission must be entered into a model, and this adds the complexity of including expert opinions but enables us to evaluate the effectiveness of the measures and mission using a single metric. When this level of awareness is required, the above models or the models that examine the attack graph in unknown attacks [7] are not comparable with our proposed model. Rather, they are parts of the problem inputs to answer a more fundamental question.

In [20], different information has been considered, focusing on the question of which countermeasure is more suitable. However, it does not provide a model with a more specific definition since it does not consider the impact on the mission. This means that it does not take into account how much the choice of an appropriate countermeasure affects the mission and the complex relationships that we consider.

Suppose you have provided various open-source services or organizational services that investigate and find vulnerabilities and CVEs in your network. You should prioritize existing CVEs. So, you can see the impact of CVEs on each other and on the mission using the proposed metric, find out how much your tasks and mission are at risk, and notice the impact of fixing each vulnerability on your mission.

Furthermore, suppose you have been attacked. You can check the impact of the attack on your mission with the data from the sensors in the network, such as IDS/ IPS. You will find out which countermeasure is more appropriate by examining the impact of different countermeasures.

5. Conclusion and Future Work

This paper provides a model to measure the effectiveness of cyber security events by employing a network dependency graph and mission dependency graph. The proposed model can help to reach a higher level of cybersecurity situational awareness.

However, the idea of the proposed model can be improved. The hierarchy tree of the model has some similarities to the neural network models. Hence, the weights might be obtained using a neural network algorithm if there existed a dataset of the services states as the input of the problem and the mission effectiveness as the output of the model. However, the main problem is the absence of such a dataset. If there existed a dataset that specified the status of the services of a mission from the beginning as input X and the effectiveness of the mission as Y, a machine learning model could be trained on this dataset, and it could be argued that it could model any dependency based on the universal approximation theorem [21]. However, each organization must have its special model, as such a dataset is not available. Moreover, each organization uses different services differently, so a database might have a different meaning for one organization than another.

The initial weights are first set by getting ideas from the models of forming the mission dependency graph and based on the experience of specialists and stakeholders to develop this model. Feedback can then be received from system users over time by implementing the model and based on the effectiveness of the services in different conditions and the specified output for mission effectiveness. The dataset might be created and completed based on the received feedback, and the model corrects any possible human error in selecting the weights by updating the weights based on this dataset. In this way, the output would be closer to the organization's desired output.

6. References

[1] Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. Human factors, 37(1), 32-64.

[2] Malowidzki, M., Hermanowski, D., & Berezinski, P. (2019). TAG: Topological Attack Graph Analysis Tool. 2019 3rd Cyber Security in Networking Conference (CSNet).

[3] Aissa, A., Abdalla, I., Hussein, L., & Elhadad, A. (2020). A novel stochastic model for cybersecurity metric inspired by Markov chain model and attack graphs. International Journal of Scientific & Technology Research, 6330– 6335.

[4] Frigault, M., & Wang, L. (2008). Measuring Network Security Using Bayesian Network-Based Attack Graphs. 2008 32nd Annual IEEE International Computer Software and Applications Conference, https://doi.org/10.1109/compsac.2008.88

[5] Khosravi-Farmad, M., & Ghaemi-Bafghi, A. (2020). Bayesian Decision Network-Based Security Risk Management Framework. Journal of Network and Systems Management, 28(4), 1794–1819.

[6] Chung, C. J., Khatkar, P., Xing, T., Lee, J., & Huang, D. (2013). NICE: Network intrusion detection and countermeasure selection in virtual network systems. IEEE transactions on dependable and secure computing, 10(4), 198-211.

[7] Wang, L., Jajodia, S., Singhal, A., & Noel, S. (2010). k-Zero Day Safety: Measuring the Security Risk of Networks against Unknown Attacks. Computer Security – ESORICS 2010, 573–587. https://doi.org/10.1007/978-3-642-154973_35.

[8] Albanese, M., & Jajodia, S. (2018). A graphical model to assess the impact of multi-step attacks. The Journal of Defense Modeling and Simulation, 15(1), 79-93.

[9] Motzek, A., & Moller, R. (2017). Context-and bias-free probabilistic mission impact assessment. Computers & Security, 65, 166-186.

[10] Kheir, N., Cuppens-Boulahia, N., Cuppens, F., & Debar, H. (2010). A service dependency model for cost-sensitive intrusion response. In Computer Security–ESORICS 2010: 15th European Symposium on Research in Computer Security, Athens, Greece, September 20-22, 2010. Proceedings 15 (pp. 626-642). Springer Berlin Heidelberg.

[11] Tadda, G. P., & Salerno, J. S. (2009). Overview of Cyber Situation Awareness. Advances in Information Security, 15–35. https://doi.org/10.1007/978-1-44190140-8_2

[12] Zand, A., Houmansadr, A., Vigna, G., Kemmerer, R., & Kruegel, C. (2015, December. Know Your Achilles' Heel: Automatic Detection of Network Critical Services, in Proceedings of the 31st Annual Computer Security Applications Conference (pp. 41-50).

[13] Yang, T., Shen, J., Su, Y., Ling, X., Yang, Y., & Lyu, M.R. (2021, November). AID: Efficient Prediction of Aggregated Intensity of Dependency in Largescale Cloud Systems. In 2021 36th IEEE/ACM International Conference on Automated Software Engineering (ASE) (pp. 653-665). IEEE.

[14] Yin, J., Zhao, X., Tang, Y., Zhi, C., Chen, Z., & Wu, Z. (2016). Cloudscout: A non-intrusive approach to service dependency discovery. IEEE Transactions on Parallel and Distributed Systems, 28(5), 1271-1284.

[15]. FarahaniNia, S., Dehghan, M., Sadeghiyan, B., and Niksefat, S. (2023), Impact Assessment for Cyber Security Situation Awareness, International Journal of Information and Communication Technology Research, 15(3), 21-30.

[16] Shirazi, A., Kazemi, M. (2020). A New Model for Information Security Risk Management. In: Baghdadi, Y., Harfouche, A., Musso, M. (eds) ICT for an Inclusive World. Lecture Notes in Information Systems and Organisation, 3 551-566.

[17] Rongrong, X., Xiaochun, Y., Zhiyu, H. (2019). A Framework for Risk Assessment in Cyber Situational Awareness. IET Information Security. 13(2), 149-156.

[18] Saaty, T. L. (1988). What is the analytic hierarchy process? Springer Berlin Heidelberg, 109-121.

[19] Saaty, T. L., Vargas, L. G., Saaty, T. L., & Vargas, L. G. (2013). The analytic network processes. Springer US.

[20] Doynikova, E., & Kotenko, I. (2016). Countermeasure selection based on the attack and service dependency graphs for security incident management. In Risks and Security of Internet and Systems: 10th International Conference, CRiSIS 2015, Mytilene, Lesbos Island, Greece, July 20-22, 2015, Revised Selected Papers 10 (pp. 107-124). Springer International Publishing.

[21] Hornik, K., Stinchcombe, M., & White, H. (1989). Multilayer feedforward networks are universal approximators. Neural networks, 2(5), 359-366.