Chapter

Risk Assessment in IT Infrastructure

Bata Krishna Tripathy

Abstract

Due to large-scale digitization of data and information in various application domains, the evolution of ubiquitous computing platforms and the growth and usage of the Internet, industries are moving towards a new era of technology. With this revolution, the IT infrastructure of industries is rapidly undergoing a continuous change. However, the insecure communication channel; intelligent adversaries in and out of the scene; and loopholes in the software and system development add complexity in deployment of the IT infrastructure in place. In addition, the heterogeneous service level requirements from the customers, service providers, users, along with implementation policies in industries add complexity to this problem. Hence, it is necessary to assess the risk associated with the deployment of the IT infrastructure in industries to ensure the security of the assets involved. In this chapter, we present an efficient risk assessment mechanism in IT infrastructure deployment in industries, which ensures a strong security perimeter over the underlying organizational resources.

Keywords: IT infrastructure, loopholes, service level requirements, common vulnerability scoring system (CVSS), vulnerability, exposure, threat, risk

1. Introduction

In today's world, every industry has their own business goals and functions. In this digital era, industries completely rely on automated information technology (IT) systems to process and manage their typical information to achieve their business objectives. The large-scale digitization of data and information across the various domain, the evolution of ubiquitous computing platforms and growth and usage of the Internet have steered the deployment of information technology systems in industries. IT infrastructure enables efficient service provisioning to end users from various enterprise applications based on Service Level Agreements (SLAs) and dynamic requirements in terms of policies by maintaining the global view of the system. Hence, information technology has become the economic backbone of any industry and offers significant advantages in global markets.

Information technology in an organization includes heterogeneous entities such as general-purpose computing systems, specialized control systems, communication network entities, database management systems, and various software control modules. The integration of these diverse entities helps in the growth and development of an organization by providing reliability, efficiency and robustness of typical information systems as well as business process flow. Despite the advantages

provided by the implementation of IT in organizations, open access-control by different levels of users, ubiquitous execution of software modules and control management introduce various security threats. These threats open the door for potential vulnerabilities, environmental interruptions, and inevitable errors leading to different cyber attacks. These attacks can extend to Denial of Service (DoS), code injection, and hidden tunnel, etc. As a result of various attacks, the confidentiality, integrity, availability (CIA) of the critical information is severely compromised. This, in turn, may have a huge impact on organizational assets, business operations, individuals, other stakeholders, and above all the Nation's assets.

Researchers have witnessed that as compared to outside threats there are pre-eminent threats from inside users and entities in organizations [1]. The organizations must understand the importance and responsibilities for protecting critical organizational information, assets, and processes from intelligent attackers. It has become an imperative duty of the organization for assessing the risk associated with the operation and use of different entities in information technology systems. Risk assessment is a key discipline for making effective business decisions by identifying potential managerial and technical problems in IT infrastructure. Then, necessary remediation can be taken by the managers of the organization to minimize or eliminate the probability and impact of these problems.

This chapter presents an efficient risk assessment mechanism that proactively analyzes the risks of IT infrastructure creating strong isolation between different entities. The proposed risk assessment solution determines the threat associated with different entities by analyzing vulnerability and exposure with respect to the Common Vulnerability Scoring System (CVSS) [2]. The overall risk of the IT systems is calculated as the cumulative threat values of different entities. These risk measures, in turn, drive the remediation process for appropriate risk mitigation in the organization strengthening the security perimeter of the organizational resources.

The rest of the chapter is organized as follows. Section 2 presents the related works in risk assessment in IT infrastructure. Section 3 presents the background of the risk assessment of IT infrastructure in organizations. The steps of risk assessment are discussed in Section 4. Section 5 presents our proposed IT risk assessment framework in detail. Section 6 summarizes the chapter.

2. Related works

Security risk assessment in enterprise networks has ever remained a major challenge for research communities. Defining security metrics play an important role in risk assessment. The literatures [3–5] define various security metrics. The effectiveness of a risk assessment mechanism relies on the security metric considered during the risk evaluation process.

The primitive risk management mechanisms were qualitative-based which used the System Security Engineering-Capability Maturity Model (SSE-CMM) using attack graphs [6]. However, these works do not evaluate risk quantitatively which can play a major role in identifying several threats. Later, the Common Vulnerability Scoring System (CVSS) [2] was proposed which is used for quantitative risk evaluation. VRSS [7] is another quantitative approach that evaluates risk using varieties of vulnerability rating systems. This uses statistics from different vulnerability databases such as IBM ISS X-Force, Vupen Security, and National Vulnerability database to determine overall risk measure in an organization. However, these works significantly lack accurate evaluation of risk in an enterprise network because of the security metrics considered and the evaluation process.

The work [4] presents a quantitative risk assessment method that determines the threat value from the number of attacks in a specific time interval. Munir et al. [8] proposed another quantitative risk assessment method using the vulnerability scanning tool (Nexpose) to determine the vulnerability values in each node in the network. This method uses the CVSS and the probabilistic approach to determine an overall risk measure of the enterprise network. In another work [9] the risk of the network is analyzed by determining the impact and likelihood of vulnerabilities. It uses WPA2 as the basic cryptographic algorithm.

On the other hand, Guohua [10] presented a risk assessment technique based on AHP (Analytic Hierarchy Process) which quantitatively determines the confidentiality, integrity, and availability of the assets with respect to the individual asset classes. In another work, Munir et al. [11] proposed a risk assessment mechanism based on the classification of different attacks as per their characteristics. This work also implements a method using a rule in Snort NIDPS signature database and OWASP risk rating approach to determine the overall risk of an enterprise network.

In a recent work, Lamichhane et al. [12] presented a quantitative risk assessment approach which computes risk as a function of overall vulnerabilities exploitation along a path and impact of the exploitation. This work implements Topological Vulnerability Analysis (TVA) for modeling and analysis of attack paths using attack graph. Chalvatzis et al. [13] proposed a virtual machine based testing framework for the performance of vulnerability scanners of the enterprise networks. The literature presented a comparative statistics of the vulnerability scanning solutions such as Nessus, OpenVAS, Nmap Scripting Engine with respect to their automation risk assessment process.

However, the state of art works do not accurately determine the risk of the enterprise network considering the risk associated with individual assets, the impact, and criticality of the information flow. In this chapter, we present an efficient risk assessment mechanism in IT infrastructure deployment in industries which addresses the limitations of the existing risk assessment techniques. Our proposed solution ensures a strong security perimeter over the underlying organizational resources by considering the level of vulnerability, threat, and impact at individual assets as well as the criticality of the information flow in the organization.

3. Background

The managers and stakeholders of organizations must understand and identify the different parameters necessary for assessing the risk of IT infrastructure. These parameters are defined as follows.

3.1 Vulnerability

It is defined as a software and hardware level weakness in the entities of IT systems, which may allow an attacker to reduce the information assurance of the entities and the underlying network [14]. In other words, it is the source of a known problem that opens the door for a potential attack on the IT infrastructure system. For example, if the managers of an organization mistakenly do not disable the access to resources and processes such as logins to internal systems for an ex-employee, then this leads to both unexpected threats to the IT infrastructure. In most cases, the vulnerabilities are exploited intentionally or unintentionally by inside or outside users of the IT systems and have a severe impact on the organizational assets. Hence, identifying weak points in the entities of IT systems is the first

step to managing the risk of the IT infrastructure to ensure reliability, robustness, efficiency, and security of IT resources.

3.2 Exposure

It is defined as the state or condition of a system being unprotected and open to the risk of suffering the loss of information [15]. In general, exposure of an entity may be a malicious piece of code, commands, or open-source tools that may potentially cause system configuration issues. This, in turn, may allow attackers to track business process flow as well as to gather critical information and at far can lead to gain access to even whole IT infrastructure. Determining exposure is the primary objective of an attacker for discovering a vulnerability in the IT systems. Generally, the exposure of an entity in the IT systems is represented as the ratio of the potentially unprotected portion of the entity to the total entity size.

3.3 Threat

Threats are potential events for vulnerabilities that might lead to exposure of the network and adversely impact the organizational assets [16]. A threat has the potential of causing small to even severe damage to the IT infrastructure of organizations. The source or root of threats can be natural, intentional or unintentional. Natural threats can be catastrophe such as floods, cyclones, earthquakes, etc. On the other hand, unintentional threats can be mistakes done by employees of organizations such as accessing the wrong resources. Intentional threats are created by attackers by flooding malicious codes over the network in the form of spyware, malware, worms, viruses, etc. Most recently, on Oct 24, 2019, Ransomware and DDoS attacks brought down major banks in South Africa including Johannesburg demanding a ransom of four Bitcoins that is equivalent to about R500,000 South African Rand or $37,000 USD [17]. Vulnerability and exposure of an entity are used to determine its threat value.

3.4 Risk

It is defined as an uncertain incident created as a result of a system malfunction and in turn has a severe impact on organizational assets and business objectives [18]. In general, the risk is a qualitative measure of potential security threat and its impact on the network [19]. In other words, the risk is defined as the potential for harm to organizations' resources when a vulnerability is exploited to threat. For example, the risk may include loss of privacy, financial loss, legal complications, etc. Hence, the overall risk of the IT systems is assessed by analyzing the vulnerability, exposure, and threat of different entities in the IT infrastructure.

Risk assessment plays a key role in making and implementing effective business decisions by proactively identifying potential problems at different managerial and technical levels. Risk management, therefore, can follow necessary remediation steps to overcome the severity of these problems [20].

4. Steps for IT risk assessment

An effective IT risk assessment process in an organization comprises the following major steps or phases. These steps are similar to the steps illustrated in the work [21]. However, we have considered the sub-phases of the evaluation phase, that is,

identifying vulnerabilities, determining exposure, determining threat as different phases in our work since these steps are equally important as compared to other phases. The risk assessment process follows a life cycle with these steps or phases as shown in **Figure 1** aiming to eliminate or minimize the level of risks in the IT infrastructure.

4.1 Step 1: Evaluation

In this phase, the critical resources that may have potential vulnerability and have threats must be understood and identified. The critical resources include the process flows, enterprise information, and assets in the IT infrastructure that are important for the functioning and security of the business. This, in turn, helps in understanding the consequences of critical information loss and in decision making regarding the resources that need to be protected.

4.2 Step 2: Identifying vulnerabilities

In this phase, the inherent vulnerabilities in the entities of IT systems are reviewed, identified and listed that have potential threats to affect the organizational assets and business process. This includes both software and hardware-level vulnerabilities of IT infrastructure. The list of vulnerabilities must have detailed information such as type, impact, measure, etc.

4.3 Step 3: Determining exposure

In this phase, the exposure of the entities in the IT systems that may have a potential threat to different attacks is determined and reported. Generally, the exposure of an entity in the IT systems is computed as the ratio of the potentially unprotected portion of the entity to the total entity size.

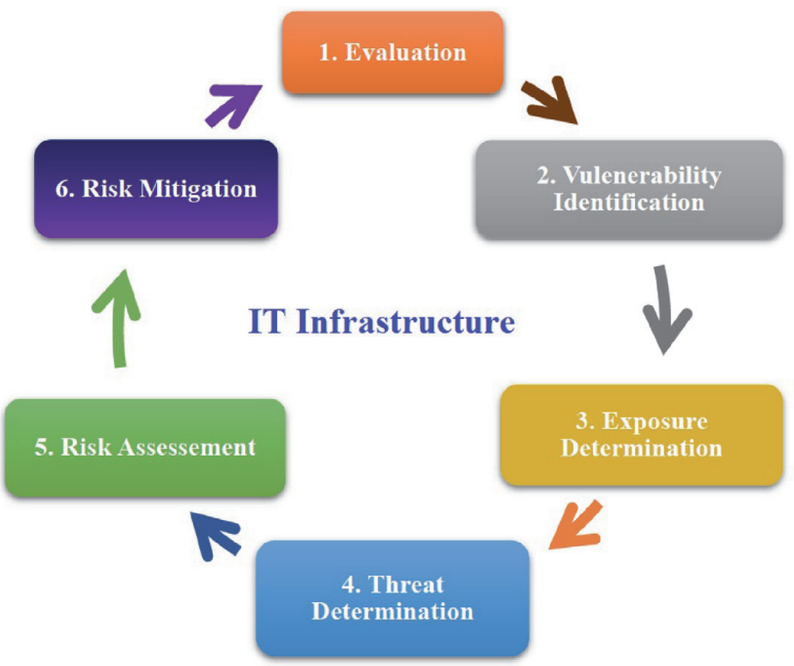

Figure 1.
Risk assessment life cycle in IT infrastructure.

4.4 Step 4: Determining threat

In this phase, information on potential threats to the organizational assets and information is gathered that may have a direct or an indirect impact on the business process. This includes collecting details of the threats on each IT entities from inside and outside users or attackers. This ultimately guides the risk assessment process for the necessary remediation plan and action to protect the organizational resources.

4.5 Step 5: Risk assessment

This phase focuses on determining the probability and impact of the vulnerabilities in the entities of IT systems. As all threats do not have the likelihood of equal occurrence and impact on the organizations' infrastructure, so it is crucial to correctly identify different levels of risk. Hence, each level of risk is determined by mapping individual threats, exposure, and vulnerabilities of an entity based on their probability and impact to critical resources of the organization. This, in turn, helps in decision making on the implementation of appropriate remediation acts.

4.6 Step 6: Risk mitigation

Once the risk assessment is performed, the final step for IT managers is to plan and act according to take preventive measures for potential threats to the organizations. It may consist of different measures such as identifying different threats before their occurrence, minimizing or eliminating the consequences of security breaches, recovering to a safe state to resume normal business process, etc.

5. IT risk assessment framework

In this chapter, an effective IT assessment framework is presented to ensure a strong security perimeter over the vulnerable IT environment of the organizations.

5.1 Vulnerability analysis

The Common Vulnerability Scoring System (CVSS) [2] plays an important role in the risk assessment of the entities in the IT infrastructure to ensure secure business information flow across the IT systems. The risk assessment module uses a data structure called vulnerability database for this purpose. The vulnerability database is a local repository (offline) stored in the controller. It is periodically updated with the recent Common Vulnerability Score (CVS) values of the applications or protocols or services running in different hardware and software components or entities of IT infrastructure. The CVS values are computed by extracting necessary metrics from the online National Vulnerability Database (NVD) [22] using a script.

The recent vulnerability values available in NVD are in XML format which contains two standard scores: V2 and V3 in the form of Common Vulnerability and Exposure (CVE) measures. The detailed process of parsing CVE values from NVD and storing in the local vulnerability database as CVS values is explained in **Figure 2**. It is to be noted that in the vulnerability database, there exists exactly one entry of CVS value for an application with its version and the Operating System platform as it is the updated CVSS value of the application parsed from NVD's recent XML file using the script. The structure of an entry in the vulnerability database is <*Application/service/protocol*, *Version*, *Operating system*, *CVS value*>.

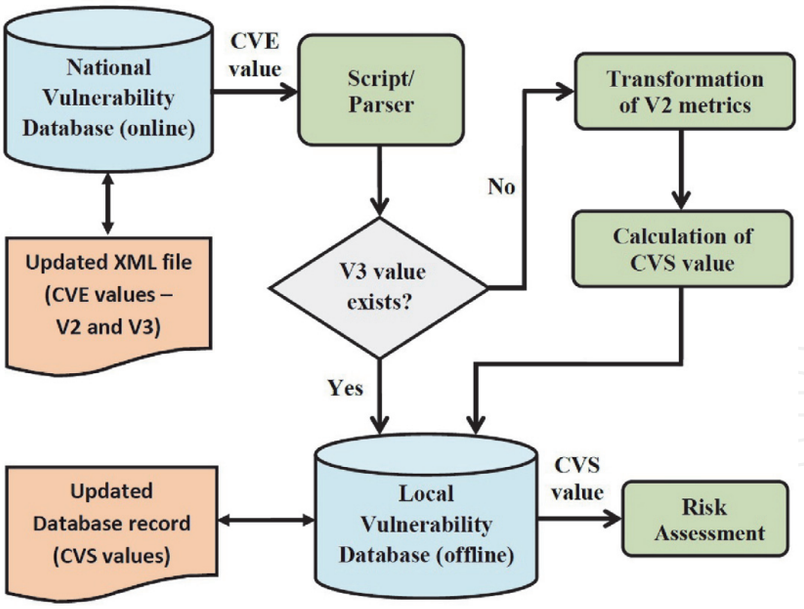

Figure 2.
Parsing CVE values from NVD and storing as CVS values in local vulnerability database for risk assessment.

Generally, the V3 standard is an improvement over the V2 standard as V3 considers the context of attacker's access rights to read/write/execute to exploit the vulnerability and physical manipulation of the affected components. Hence, the risk assessment module uses the V3 version of CVE as its CVS value for necessary risk assessment for secure business processes and information flow. However, for some older vulnerabilities there exist only V2 values in NVD. In such a case, the CVS value for a vulnerability is calculated in two steps from the available V2 metrics in NVD as discussed below.

5.1.1 Step 1: Transformation of V2 metrics

To compute the overall vulnerability value, CVSS considers certain metrics that define the hardware, software and network-level vulnerabilities in the IT systems. The V2 version differs from the V3 version in terms of the metrics and their values considered for overall vulnerability score computation. However, for some older vulnerabilities, V3 value is not available in the NVD. In this scenario, the CVS value for a vulnerability in our solution is estimated from the V2 metrics available in the XML file by appropriately transforming the metrics and their values as shown in **Table 1**. The transformation is performed as per the CVSS V2 and V3 standards [23, 24].

These metrics after the transformation process are then used for the necessary CVS computation in the proposed mechanism. The estimation of CVS value for a vulnerability is performed as explained below in the subsequent step.

5.1.2 Step 2: Calculation of CVS values

The CVS value for a vulnerability is determined from the desired metrics obtained in the previous step, using the standard equations for the overall V3 version of CVSS computation [24] with optimization to minimize the overhead of the CVS computation process. The procedure of the overall CVS value calculation is illustrated in **Figure 3**.

The entities of the IT infrastructure might be the potential sources of vulnerabilities in the organization. Hence, the vulnerability of each entity is determined by

V2 metric		Value	Transformed metric	Value
Base metrics				
Exploitability group	Access vector	Local: 0.395	Attack vector	Local: 0.55
		Adjacent network: 0.646		Adjacent: 0.62
		Network: 1.0		Network: 0.85
	Access complexity	High: 0.35	Attack complexity	High: 0.44
		Medium: 0.61		Medium: 0.62
		Low: 0.71		Low: 0.77
	Authentication	Multiple: 0.45	Privileges required	High: 0.27
		Single: 0.56		Low: 0.62
		None: 0.704		None: 0.85
Impact group	Confidentiality, integrity, and availability	None: 0.0	Confidentiality, integrity, and availability	None: 0.0
		Partial: 0.275		Low: 0.22
		Complete: 0.66		High: 0.56
Temporal metrics				
	Exploitability	Unproven: 0.85	Exploitability	Unproven: 0.91
		Proof-of-concept: 0.9		Proof-of-concept: 0.94
		Functional: 0.95		Functional: 0.97
		High: 1.0		High: 1.0
	Remediation level	Official fix: 0.87	Remediation level	Official fix: 0.95
		Temporary fix: 0.90		Temporary fix: 0.96
		Workaround: 0.95		Workaround: 0.97
		Unavailable: 1.0		Unavailable: 1.0
	Report confidence	Unconfirmed: 0.90	Report confidence	Unknown: 0.92
		Uncorroborated: 0.95		Reasonable: 0.96
		Confirmed: 1.0		Confirmed: 1.0
Environmental metrics				
General modifiers	Collateral damage potential	None: 0	Attack vector	None: 0
		Low (light loss): 0.1		Physical: 0.2
		Low-medium: 0.3		Local: 0.55
		Medium-high: 0.4		Adjacent network: 0.62
		High (catastrophic loss): 0.5		Network: 0.85
	Target distribution	None: 0	Attack complexity	None: 0
		Low: 0.25		Low: 0.77
		Medium: 0.75		Medium: 0.62
		High: 1.0		High: 0.44

V2 metric		Value	Transformed metric	Value
Impact subscore modifier	Confidentiality, integrity, and availability requirements	Low: 0.5	Confidentiality, integrity, and availability requirements	Low: 0.5
		Medium: 1.0		Medium: 1.0
		High: 1.51		High: 1.5

Table 1.
Transformation of V2 metrics and their values for CVS computation.

the above-mentioned steps. Then, the threat for different entities is determined using the threat model using vulnerability and exposure analysis of those entities. Then, the overall risk of the IT systems is determined as cumulative threat values of the entities and criticality of the business process and information flow.

5.2 Threat model

In this phase, the threat associated with different IT entities is modeled using the vulnerability and exposure of the entities as follows.

5.2.1 Vulnerability of an entity

Several vulnerable applications, services or protocols such as FTP, RSH, Nmap, etc. may be running in an IT entity for the functioning of business processes. The vulnerability V_e of an entity e is calculated as the average of the Common Vulnerability Scores (CVS) of all the applications running on the entity extracted from the vulnerability database, that is,

$$V_e = \frac{1}{10} * \frac{\sum_{i=1}^{k} CVS_i}{k} \tag{1}$$

where CVS_i is the Common Vulnerability Score of the ith application or protocol or service running in the entity e, and k is the number of applications, protocols, and/or services running in the entity. The average value of the CVS of all applications, protocols and/or services is divided by 10 to normalize the value of V_e to 1 as the CVS lies between 0 and 10.

5.2.2 Exposure of an entity

The exposure E_e of an entity e is determined considering the number of entities that may be affected because of the vulnerability in the target entity. Hence, it is computed as,

$$E_e = \frac{n}{N} \tag{2}$$

where n is the number of entities communicating with the target entity and N is the total number of entities in the IT systems.

The vulnerability values and threat models guide the risk assessment process for estimating risk levels of the entities in the IT infrastructure.

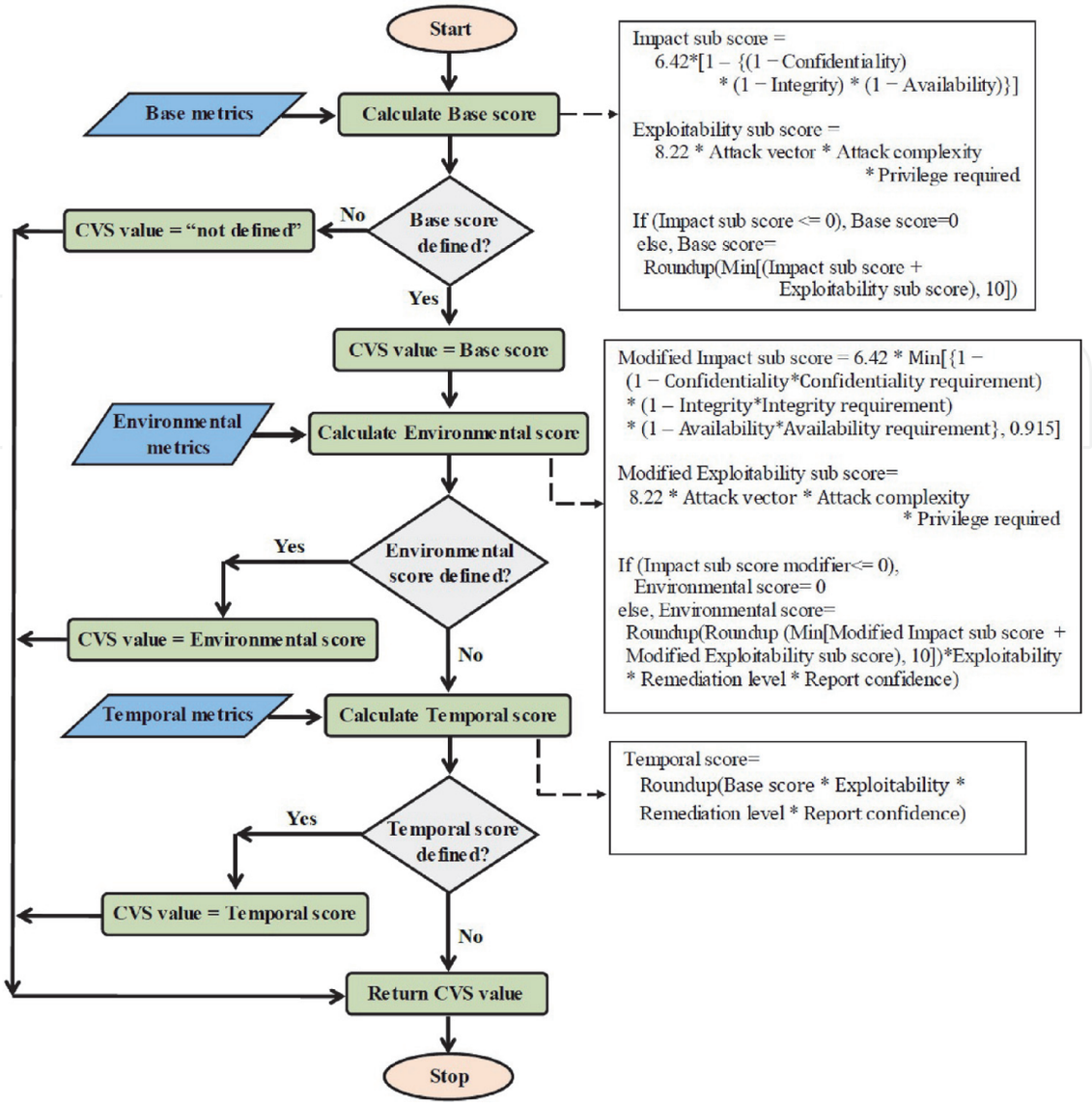

Figure 3.
CVS computation of vulnerabilities from the transformed metrics in case of nonavailability of V3 value in NVD.

5.3 Risk assessment model

The risk assessment model first evaluates the threat model for different IT entities as discussed in the previous subsection. Then, the overall threat value τ is calculated as the cumulative threat values of all the entities in the IT systems involved in the business process flow. Algorithm 1 illustrates the risk assessment procedure to determine the overall threat value τ.

Algorithm 1 uses weight w_e for each entity in order to consider the criticality of different entities and should be chosen such that their sum must be equal to 1, that is,

$$\sum w_e = 1 \tag{3}$$

In our work, we have used the term *weight* as it is a quantitative term instead of the term *criticality* which is usually a qualitative term.

The overall threat value (τ) and its criticality (I) of business process and information flow are used to define the overall risk (R) of the entities in IT systems. The criticality of the business process and information flow can be high (H),

Algorithm 1 *Risk assessment* algorithm

```
procedure RISK_ANALYZE
    Entity set E= e1, e2, ... , en
    for each entity e ∈ E do
        find Ve
        find Ee
        calculate τe=Ve*Ee
    end for
    calculate τ= ∑ we*τe
end procedure
```

medium (M) or low (L). The criticality of a business process and information flow depends on the impact of the business process and information flow in a specific application context. For example, in a banking application, transactions have high impact and hence have High importance whereas the generation of logs has medium impact leading to medium importance. On the other hand, simple query processing has a low impact on the context and hence has low importance. So, we consider three different criticality levels; that is, high (H), medium (M) and low (L), respectively for these three types of business process and information flow.

The mapping function for assessing the risk of a specific business process and information flow is expressed as:

$$f : \tau \times I \rightarrow R \tag{4}$$

Table 2 shows the risk assessment model of IT infrastructure with respect to the criticality and threat level of the specific business process and information flow in the enterprise network. For example, in a banking application, transactions have high impact and hence have high criticality whereas the generation of logs has medium impact leading to medium criticality. On the other hand, simple query processing has a low impact on the context and hence has low criticality. So, we consider three different criticality levels of the business process and information flow; that is, high (H), medium (M) and low (L), respectively for overall risk assessment. For example, if the criticality of a business process and information flow is high (H) and its threat value is 5.5, then the risk associated with the business process and information flow is high (H). Similarly, individual risk levels are determined concerning specific business processes and information flow.

The calculated risk measures determined by the risk assessment model, are used in decision making and remediation planning for protecting the systems against different potential attacks. This process is executed recursively to eliminate or minimize the level of risks in the IT infrastructure.

Criticality of business process and information flow	**Total threat value**		
	⩽0.39	**0.4 to 0.69**	**⩾0.7**
H	M	H	C
M	L	M	H
L	L	L	M

Note: C, critical; H, high; M, medium; and L, low.

Table 2.
Risk assessment model of IT infrastructure.

6. Conclusion

The evolution of ubiquitous computing systems has steered the industries towards relying on IT infrastructure for their business operations. In addition, industries are competing in the global market adapting to the rapid and continuous changes in IT systems. However, deployment of the IT infrastructure across industries has always remain complicated because of the insecure communication channel; intelligent inside and outside attackers; and loopholes in the software and system development life cycle. In addition, the heterogeneous service level requirements from the customers, service providers, users, along with implementation policies in industries add complexity to this problem. Hence, effective assessment of risk associated with the deployment of the IT infrastructure in industries has become an integral part of the management to ensure the security of the assets. In this chapter, an efficient risk assessment mechanism for IT infrastructure deployment in industries is proposed which ensures a strong security perimeter over the underlying organizational resources by analyzing the vulnerability, threat, and exposure of the entities in the system.

Abbreviations

IT	information technology
NVD	National Vulnerability Database
CVSS	Common Vulnerability Scoring System
CVS	Common Vulnerability Score
CVE	Common Vulnerability and Exposure

Author details

Bata Krishna Tripathy
Indian Institute of Technology Bhubaneswar, India

*Address all correspondence to: bata.krishna.tripathy@gmail.com

References

[1] Insider vs. Outsider Data Security Threats: What's the Greater Risk? [Online]. Available from: https://digitalguardian.com/blog/insider-outsider-data-security-threats. [Accessed: 01 November 2019]

[2] Mell P, Scarfone K, Romanosky S. Common vulnerability scoring system. IEEE Security and Privacy. 2006;**4**(6): 85-89. [Accessed: 01 November 2019]

[3] Li J, Wang H. A quantification method for network security situational awareness based on conditional random fields. In: Fourth International Conference on Computer Sciences and Convergence Information Technology; Seoul; 2009. pp. 993-998. [Accessed: 01 December 2019]

[4] Breu R, Innerhofer-Oberperfler F, Yautsiukhin A. Quantitative assessment of enterprise security system. In: Third IEEE International Conference on Availability, Reliability and Security; Barcelona; 2008. pp. 921-928. [Accessed: 01 December 2019]

[5] Xie A et al. An adjacency matrixes-based model for network security analysis. In: IEEE International Conference on Communications; Cape Town, South Africa; 2010. pp. 1-5. [Accessed: 01 December 2019]

[6] Noel S et al. Measuring security risk of networks using attack graphs. International Journal of Next Generation Computing. 2010;**1**(1): 135-147. [Accessed: 01 December 2019]

[7] Liu Q, Zhang Y. VRSS: A new system for rating and scoring vulnerabilities. Computer Communications. 2011;**34**: 264-273. [Accessed: 01 December 2019]

[8] Munir R, et al. A quantitative measure of the security risk level of enterprise networks. In: Eighth IEEE International Conference on Broadband and Wireless Computing, Communication and Applications; Compiegne; 2013. pp. 437-442. [Accessed: 01 December 2019]

[9] Liang L, et al. The practical risk assessment for enterprise Wireless Local Area Network. In: IEEE International Conference on Information Science, Electronics and Electrical Engineering; Sapporo; 2014. pp. 1936-1940. [Accessed: 01 December 2019]

[10] Guohua Z. Enterprise information security risk and countermeasure research under network environment. In: Seventh IEEE International Conference on Measuring Technology and Mechatronics Automation; Nanchang; 2015. pp. 453-456. [Accessed: 01 December 2019]

[11] Munir R, et al. Detection, mitigation and quantitative security risk assessment of invisible attacks at enterprise network. In: 3rd IEEE International Conference on Future Internet of Things and Cloud; Rome; 2015. pp. 256-263. [Accessed: 01 December 2019]

[12] Lamichhane PB, Hong L, Shetty S. A quantitative risk analysis model and simulation of enterprise networks. In: 9th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON); Vancouver, BC; 2018. pp. 844-850. [Accessed: 01 December 2019]

[13] Chalvatzis I, Karras DA, Papademetriou RC. Evaluation of security vulnerability scanners for small and medium enterprises business networks resilience towards risk assessment. In: IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA); Dalian, China; 2019. pp. 52-58. [Accessed: 01 December 2019]

[14] Vulnerability (Computing), Wikipedia [Online]. Available from: https://en.wikipedia.org/wiki/Vulnerability_(computing). [Accessed: 01 November 2019]

[15] Exposure [Online]. Available from: http://www.businessdictionary.com/definition/exposure.html. [Accessed: 01 November 2019]

[16] Threat (Computer), Wikipedia [Online]. Available from: https://en.wikipedia.org/wiki/Threat_(computer). [Accessed: 01 November 2019]

[17] Cyber Attacks Hit the City of Johannesburg and South African Banks [Online]. Available from: https://www.thesslstore.com/blog/cyber-attacks-hit-the-city-of-johannesburg-and-south-african-banks/. [Accessed: 01 November 2019]

[18] Harvey J, Technical Information Service. Introduction to Managing Risk [Online]. Available from: http://www.cimaglobal.com/Documents/Imported Documents/cid_tg_intro _to_managing_rist.apr07.pdf. [Accessed: 01 November 2019]

[19] Cybersecurity Risk: A Thorough Definition, Bitsight [Online]. Available from: https://www.bitsighttech.com/blog/cybersecurity-risk-thorough-definition. [Accessed: 01 November 2019]

[20] Georgieva K, Farooq A, Dumke RR. Analysis of the risk assessment methods —A survey. In: Software Process and Product Measurement. IWSM 2009. Lecture Notes in Computer Science, Vol. 5891. Berlin, Heidelberg: Springer

[21] IT Risk Assessment—Happiest Minds [Online]. Available from: https://www.happiestminds.com/whitepapers/IT-risk-assessment. [Accessed: 01 November 2019]

[22] National Vulnerability Database (NVD) [Online]. Available from: https://nvd.nist.gov/ [Accessed: 01 November 2019]

[23] A Complete Guide to the Common Vulnerability Scoring System Version 2.0 [Online]. Available from: https://www.first.org/cvss/v2/guide. [Accessed: 01 November 2019]

[24] Common Vulnerability Scoring System v3.0: Specification Document [Online]. Available from: https://www.first.org/cvss/specification-document. [Accessed: 01 November 2019]