

Efficacy and Security Effectiveness: Key Parameters in Evaluation of Network Security

S. Guru Prasad^{a,*}, M. K. Badrinarayanan^a, and V. Ceronmani Sharmila^b

^a*School of Management, Hindustan Institute of Technology & Science, Chennai, 603103, India*

^b*Department of Information Technology, Hindustan Institute of Technology & Science, Chennai, 603103, India*

Abstract

Information is the most critical asset of modern-day organisations. Organisations use various information technology tools, products, and solutions to store the information. Because of its importance to organisations, information is protected using various information protection tools, that would include computer or network hardware and software. This article aims to give the organisations and their Chief Information Security officers a template for technical evaluation of the various network security solutions with Security effectiveness as a key element in their decision making.

Keywords: network security; effective network security; network security components; template for network security evaluation; network security evaluation by CISOs

(Submitted on January 18, 2022; Revised on February 15, 2022; Accepted on March 13, 2022)

© 2022 Totem Publisher, Inc. All rights reserved.

1. Introduction

Various Techniques which are being used to send, receive, store, retrieve and analyze of all kinds of data, voice, and Video are referred as Information Technology (IT). Information Technology uses various computer hardware, software and associated components and processes to manage and operate a range of technological processes. In most organisations, computer hardware and software are connected to each other to form a network of computers so that information can be shared.

Information Technology (IT) is one of the most important resources used for business information management. These resources include hardware, software, and communication networks used for information management [1]. The introduction of an integrated Information Technology enabled business system makes a company well- equipped to deliver better services to their customers [2]. Information technology growth and its importance has brought in newer opportunities for the benefit of modern society [3]. With more and more organisations adopting Information technology networks for business enhancements, the attacks on these Information technology networks, and resources have also increased. Information is a critical resource of every organization which needs to be protect from both internal and external threats [4]. Information Security threats in any organisation occur during storage, processing, and communication of information [5].

2. Information Security Policy & Management

Organizations develop and implement information system security policies (ISSP) as a comprehensive solution to information system security. Information security policy is a formal document that describes acceptable and unacceptable terms of behavior of users while accessing organizational information and IT resources [6].

For ensuring comprehensive protection, comprehensive security policy is a must and has to be formulated and implemented [4]. There are many guidelines and standards organisations follow for Information Security Management. ISO is an international organisation for standardization and is an independent, non-governmental international organisation with 165 national standards bodies as members [7].

* Corresponding author.
E-mail address: guru@cybertracs.in

ISO27001:2013 is widely used by organisations to create their Information Security Management Systems and its compliance is ensured by a 2 stage well established and documented audit process. However, these standards do not give guidelines on the security effectiveness.

3. Network security threats & cyber attacks

Cyber-attacks on organisations are so dangerous to the extent that it can bring in losses to organisations and sometimes bring down a company. A few examples of such cases are listed below:

- 1) The British foreign exchange company Travelex was forced to shut down due to hackers [8].
- 2) Code Space was a code hosting company. It was offering project management tools to its customers. The company faced a Distributed Denial of Service (DDoS) attack in June 2014 that caused a major disruption to their services. They also did another attack on their databases and wiped off their data backups and configurations. This attack made the firm to move out of its operations due to the very high costs of recovery from the attacks. The firm confirmed the reasoning behind their shut down in a disclosure [9].
- 3) An American healthcare provider, Wood Ranch Medical, shut down its operations and services due to a cyber-attack in 2019. The facility suffered a major cyber- attack using Ransomware in August 2019. It locked them out of their patients' data. According to reports, the attack caused major damages beyond repair to the infected systems making file recovery impossible [10].
- 4) Cosmos Bank Cyber Attack in Pune - In 2018, Cosmos bank in Pune faced a major attack when hackers siphoned off Rs. 94.42 Crores [11].

With the increase in attacks on the Information Technology Infrastructure worldwide, it has become extremely important for organisations to adopt innovative and rigorous procedures to protect their valuable Information Technology assets. In order to protect their Infrastructure from cyber-attacks and information and Data Security threats, the organisation should be implementing information security solutions on devices in their networks. Information security implementation and its management have become very important for organisations. Many organisations are turning to Information Security Managements systems to achieve Information Security requirements of their organisation and/or the legal compliances of the local land. The aim of this paper is to provide an evaluation template for the Chief Information Security Officers (CISOs) who are employed in organisations to ensure that the network is safe and Secure from any attacks.

4. Addressing the information security challenges

Modern information-gathering devices must be deployed by organisations to address their security challenges [3]. Organisations use Information security management (ISM) guidelines, which serves as a guideline to provide the best ISM practices. The security management guidelines need to be complied at all times. However, current guidelines which are available have two problems. Firstly, they are very generic in scope and application. Secondly, they have not been validated but are followed by an appeal to common practice, which is an unsound basis for a true standard [12]. These information Security Management guidelines and various available standards do not provide any guidelines for implementing the security solutions with the best security effectiveness.

Hence, most organisations buy some of the solutions and devices available in the market and implement it, which help the organisations in managing their information security. While implementing these solutions, organisations tend to find out what is available in the industry and the buy them and implement it. Sometimes they tend to buy solutions recommended by some vendors or sometimes their buying decision is influenced by the budget they have or by any analyst/customer reference. In most cases, the decision on the Technology & Solutions for the Network Security is done by the Chief Information Security Officer (CISO). Hence, there can be a potential gap between Information Security requirements of the organisation, risk faced by the organisation, threat landscape, and what is implemented in the organisation.

Network Security Solutions: To address this gap, we studied various Network Security Solutions available in the industry. We shortlisted the solutions of the OEMs which are in Gartner Magic Quadrant. We studied those solutions which are in the Leader Quadrant of the Gartner Magic Quadrant to study what all the Network Security components they offer and what kind of protections they provide to the organisations. Gartner's Magic Quadrant for Firewall and UTM is considered for the study [13].

The following are the Network Security Brands which are studied to analyse the Network Security hardware and Software they offer and also the parameters that they have mentioned to support their security efficacy and effectiveness.

- Check Point
- Fortinet

- Palo Alto
- Radware
- Imperva

Information publicly available in the respective brands and its products are studied. A sample of the information gathered is presented in Table 1:

Table 1. Network Security Common Vulnerabilities and Exposures (CVEs) covered & Signatures

Description	Network Security CVEs covered & Signatures		
	Brand A	Brand B	Brand C
IPS	Number of Critical CVE's covered by IPS (Dec 2014 – Dec 2019) • Total CVE: 4512 • Microsoft: 1477 • Adobe: 1544	Number of Critical CVE's covered by IPS (Dec 2014 – Dec 2019) • Total CVE: 4152 • Microsoft: 1104 • Adobe: 1801	Number of Critical CVE's covered by IPS (Dec 2014 – Dec 2019) • Total CVE: 4343 • Microsoft: 1177 • Adobe: 1518
Application Control & URL Filtering	Number of Application Signature (Till Date) • Total Application Intelligence – 8,600+	Number of Application Signature (Till Date) • Total Application Intelligence – 4,000+	Number of Application Signature (Till Date) • Total Application Intelligence – 3,500+

Source: Compiled from Web Sources [14-18]

The Network Security appliance or the Network Security solution is implemented with an aim to provide the best of security and threat prevention to the network and the devices connected to the network. From Table 1 we can see that Brand A offers more protection than Brand B and Brand C. Hence, the effectiveness of the solution is more important in a network to ensure maximum protection against any threats. Perimeter Network security solutions deployed in organisations consists of Perimeter Firewall, Perimeter Intrusion Detection & Prevention Systems, Distributed Denial of Service (DDoS) protection, and Sandbox systems [12].

Most organisations tend to implement the following Network Security solutions in their network to prevent the external attacks.

- Firewall
- IPS- Intrusion Prevention System
- Anti-Virus Software
- Malicious Botnet Protection Software
- Uniform Resource Locator (URL) Filtering
- Application Control Software
- Distributed Denial of Service (DDoS) Solution
- Zero-Day Protection Solution

For Information security effectiveness, Brady suggested a model which included management support, security awareness, security culture, and computer self-efficacy [12]. Information Security effectiveness can be questioned because more and more organisations are experiencing information security breaches resulting in huge financial losses [19]. Many Information Security models and controls have been proposed and many of them are implemented by various organisations. However, the breaches continue. We feel that in these processes, one very important component which is being missed by the Chief Information Security Officers (CISOs) is, the “**security efficacy of the Network Security solutions and technologies and the security effectiveness that the solutions provide**” for the organisations. Information Security effectiveness in an organisation has a direct relation to the security effectiveness of the various Information security solutions and Technologies deployed and the security effectiveness that they provide to the organisation. Here we see Network security effectiveness is:

- The efficacy of the Network Security solutions
- effectiveness of the solution deployed
- Effectiveness of the security that the solution provides
- The amount of protection the solution is able to provide

Keeping in mind of the challenges faced the Chief Information Security officers (CISOs) in choosing their Network Security Solution, we propose the following evaluation metrics. These metrics will help Chief Information Security officers (CISOs) in selecting a good Network Security solution for their organisation.

We propose the following two parameters for the evaluation: Evaluation of the efficacy of the Network Security hardware & its Operating System and Evaluation of the Effectiveness of the security that the Network Security hardware &

Software provides. The below chart gives the details of the Hardware, Operating System and Security software, its parameters for evaluation along with its evaluation criteria, and success criteria.

Table 2. Technical Evaluation of the efficacy of the Network Security Hardware & it's Operating System.

Parameters	efficacy of the Network Security hardware & its Operating System	
	Evaluation Criteria	Success Criteria
Operating System (OS)	Version Nature of the OS	latest version if the OS can be updated/upgraded seamlessly to accommodate new security patches. Is the OS hardened
OS Vulnerabilities	Any Vulnerabilities exists in the Operating System	Check for the vulnerability listing in the respective brands web site and also in the below https://stack.watch/search/ https://www.cvedetails.com/
Hardware Vulnerabilities	Any Vulnerabilities exists in the Hardware	Check for the vulnerability listing in the respective brands web site and also in the below https://stack.watch/search/ https://www.cvedetails.com/

Source: Compiled by Author

Table 2 gives the parameters like Operating System (OS), OS Vulnerabilities and hardware vulnerabilities as evaluation parameters.

Every Operating System has a version and every new update to the operating systems leads to a version change which is usually denominated in alpha numeric or numeric codes as a reference. Thereby, from that we can find out if the version is the latest or older one. In some products, the Application Specific Integrated Chipsets (ASIC) are being used. In such cases the evaluation should include checking if there can be a seamless update or upgrade to the Operating System. Some Operating Systems can have vulnerabilities. This is usually reported by independent researchers and/or by the product owners. In such cases the evaluation should include checking if the vulnerability still exists or it is addressed. If the vulnerability still exists then the risk of exploiting the vulnerability exists. There are 3rd party websites which has a list of all the vulnerabilities found.

Some Network Security hardware can have vulnerabilities. This is usually reported by independent researchers and/or by the product owners. In such cases the evaluation should include checking if the vulnerability still exists or it is addressed. If the vulnerability still exists then the risk of exploiting the vulnerability exists. There are 3rd party websites which has a list of all the vulnerabilities found.

The next evaluation metrics is to technically evaluate the effectiveness of the security that the Network Security Hardware provides and the effectiveness of the security that the security software which is in the hardware provides. The various Network Security solutions/Technologies available in the industry are Intrusion Prevention System (IPS), Anti-Virus, Anti-BOT, URL Filtering, Application control, URL Filtering, Zero-day protection, Distributed Denial of Service (DDoS). Table 3 gives the details of various security solutions in the Network security, its evaluation criteria, and its evaluation methodology.

- Intrusion Prevention System (IPS)- Intrusion Prevention System prevents intrusions into the network.
- Antivirus in the network security appliances protects the network from any virus infections.
- Anti-Bot is a technology which will help to stop bad or malicious bots.
- URL Filtering - URL filtering prevents any access to harmful websites and/or banned websites.
- Application Control blocks or restricts unauthorized applications.
- Zero-Day Protection provides security against unknown malware, zero-day and targeted attacks from infiltrating networks.
- DDoS protection solution protects the infrastructure against any network and application downtime which can happen when attackers run a distributed denial of service attack.

With so many solutions and technologies for Networking security and each one of them having different security mechanism, there is a need for the evaluation of Network Security in a structured manner. For this the evaluator should have the understanding and knowledge of the various technologies and solutions in Network Security Solutions. To facilitate that, we have tabulated the Technologies/Solutions, evaluation Criteria, and evaluation methodology in a detailed manner. Furthermore, we have prepared a questionnaire leading to a "Technical Evaluation Template" given below to make the evaluation in a structured manner.

Table 3. Technical Evaluation of the effectiveness of the Security that the Network Security Hardware & Software Provides

Technologies/Solutions	Security effectiveness of the Network Security hardware & Software	
	Evaluation Criteria	Evaluation Methodology
IPS	Does it scan all the packets? Does it scan the complete packet? Does this Scan the incoming traffic? Does this scan the outgoing traffic? Does this have any packet size limitation? Number of CVEs covered by IPS	By Checking in Publicly available documents in the respective original equipment manufacturers' (OEM's) web site and/or their configuration documentation.
Anti-Virus	How many Signatures the solution has? Can it do Deep Packet Inspection? Does the solution have more than 1 Anti-Virus Engine for scanning?	By Checking in Publicly available documents in the respective original equipment manufacturers' (OEM's) web site and/or their configuration documentation.
Anti-BOT	How many BOT communication patterns detection is available in this software? How many Command-and-Control URL reputation database is present in this software?	By Checking in Publicly available documents in the respective original equipment manufacturers' (OEM's) web site and/or their configuration documentation.
URL Filtering	Total URL Database Total Number of URL Categories	By Checking in Publicly available documents in the respective original equipment manufacturers' (OEM's) web site and/or their configuration documentation.
Application Control	Total Application control Database Total Number of Application Control Categories	By Checking in Publicly available documents in the respective original equipment manufacturers' (OEM's) web site and/or their configuration documentation.
Zero-Day Protection	Does the software prevent zero-day attacks in the first attempt? Time taken to identify zero-day files? Maximum file size supported Zero-day protection engine details	By Checking in Publicly available documents in the respective original equipment manufacturers' (OEM's) web site and/or their configuration documentation.
DDoS	Network Capacity to block attack Processing capacity Time to mitigation Network layer and application layer mitigation	By Checking in Publicly available documents in the respective original equipment manufacturer's (OEM's) web site and/or their configuration documentation.

Source: Compiled by Author

Table 4: Technical Evaluation Template

Sr. No	Evaluation Questions	Brand A	Brand B
1	Is the operating system in the solution the latest?		
2	Can the operating system be upgraded for patches and updates seamlessly?		
3	Is the Operating system hardened?		
4	Are there any known vulnerabilities in the operating System? If yes, how many?		
5	Are there any known vulnerabilities in the hardware? If yes, how many?		
6	How many IPS Signature are there in the solution?		
7	Does the IPS software scan all the packets?		
8	Does the IPS scan the complete packet?		
9	Does the IPS Scan the incoming traffic?		
10	Does the IPS scan the outgoing traffic?		
11	Does the IPS have any packet size limitation?		
12	What is the Number of CVEs covered by IPS		
13	How many Signatures in the Anti-Virus software?		
14	Can the Anti-Virus software do Deep Packet Inspection?		
15	How many Anti-Virus Engines are there in this solution?		
16	How many BOT communication patterns detection is available in the Anti-BOT software?		
17	How many Command-and-Control URL reputation database is present in this Anti-BOT software?		
18	what is the total number of URL database present in the URL Filtering software?		
19	What is the total number of URL categorisation available in this URL Filtering software?		
20	what is the Total number Application control Database available in the Application control software?		
21	what is the Total Number of Application Control Categories available in the Application control software?		
22	Does the Zero-day protection solution prevent Zero day attacks in the very first attempt?		
23	what is the Time taken to identify zero-day files?		
24	what is the Maximum file size supported by this Zero-day protection solution?		
25	what are the Zero-day protection engines available in this solution?		
26	what is the DDoS solution's Network capacity to block the attack?		
27	what is the processing capacity of the DDoS solution?		
28	what is time taken to mitigate the DDoS attack by the solution?		
29	What is the capacity of the solution to do Network layer mitigation & application layer mitigation?		
30	Can it mitigate Advanced Persistent DDoS? How?		

Source: Compiled by Author

Table 4 has 30 questions on various technologies that are usually deployed in Network Security. The answers to these 30 questions will give a deeper insights into the products being evaluated. Most of the answers will be quantitative in nature. Thus, it makes a comparison easier based on the data collected.

In Table 1, a sample of the information gathered (as per questions in Table 4) is given. This gives the number of Common Vulnerabilities and Exposures (CVEs) and number of application Signatures. In Table 2, Evaluation Criteria and Success criteria for Technical Evaluation of the efficacy of the Network Security Hardware and its Operating System is given. In Table 3, Evaluation criteria and Evaluation methodology for Technical Evaluation of the effectiveness of the Security that the Network Security Hardware and Software Provides are given. In Table 4, questions for technical evaluation of the Network Security solution based on Efficacy and Security effectiveness are given. In the Table 1, Table 2, and Table 3, the information relevant to the questions in Table 4 are given. By referring to the previous tables (Table 1, Table 2, Table 3) and correlating with the information gathered in Table 4, the evaluation of the Network Security solution can be completed. Most of the information required for evaluation are available in the respective solution providers or original equipment manufacturer's website and data sheet. In some cases, if the information is not available in their website or datasheet, the same can be found in their Knowledge base, Implementation guide, their community chats, and independent research reports. Some information can be found in the Network Security product itself. Here Network Security product is referred to the combination hardware and the software in the particular product that is used in Network Security.

In every organisation, securing the network is the responsibility of the Chief Information Security Officer (CISO). The above table (Table 4) in conjunction with Table 1, Table 2, and Table 3 provides a template for evaluating the network security products and solutions. This can be filled for the brands or products under evaluation and the various evaluation parameters of the network security products can be evaluated. This template helps the Chief Information Security Officers (CISOs) in choosing the best network security for their organisations.

5. Conclusion

Network Security has transformed over the years with the change of Information technology that organisations are using for enhancing their business. With the changes in technology, there is a change in the threat vector, attack landscape and the threat actors who create and execute attacks. This paper has captured the technologies/solutions that are used in protecting the Network of Information technology devices that organisations use in their Information Technology Network. Most organisations use a number of metrics like throughput of the appliances, number of ports available, and list of technologies available in the solutions to provide protection against various attacks. This paper has given the metrics for evaluation of Network Security solutions that are typically deployed in the enterprises and various organisations. These metrics are designed with "efficacy and Effectiveness" of the Network Security solutions as the key element of evaluation. The Network Security in an organisation is as effective as the efficacy and effectiveness of the network security solution itself. The aim of this paper is to provide an evaluation template to the Chief Information Security Officers (CISOs) who are employed in organisations to ensure the Network is safe and secure from any attacks. Network Security landscape keeps on changing. As and when newer technologies get added, newer evaluation criteria have to be added.

References

1. Chaffey, Wood. Business Information Management: Improving Performance Using Information Systems. *Essex: Pearson Education Limited*, 2005.
2. Olugbode, M., Richards, R. and Biss, T. The Role of Information Technology in Achieving the Organisation's Strategic Development Goals: A Case Study. *Information Systems*, vol. 32, no. 5, pp. 641-648, 2007.
3. Yeganegi, K., Arbabi, Z., and Hussein, A.I. The Role of Information Technology in National Security. In *Journal of Physics: Conference Series*, vol. 1530, no. 1, pp. 012112, 2020.
4. Assefa, T. Factors Influencing Information Security Compliance: An Institutional Perspective. *SINET: Ethiopian Journal of Science*, vol. 44, no. 1, pp. 108-118, 2021.
5. Kim, D. and Solomon, M.G. *Fundamentals of information systems security*. Jones & Bartlett Publishers. 2018
6. Alotaibi, M., Furnell, S. and Clarke, N. Information Security Policies: A Review of Challenges and Influencing Factors. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, IEEE, pp. 352-358, 2016.
7. www.iso.org, accessed April 2022.
8. <https://www.wsj.com/articles/travel-ex-currency-exchange-network-shut-down-by-virus-attack-11577995684>, accessed April 2022.
9. <https://www.csoonline.com/article/2365062/code-spaces-forced-to-close-its-doors-after-security-incident.html>, accessed April 2022.
10. <https://www.hipaajournal.com/wood-ranch-medical-announces-permanent-closure-due-to-ransomware-attack>, accessed April 2022.

11. <https://economictimes.indiatimes.com/industry/banking/finance/banking/cosmos-banks-server-hacked-rs-94-crore-siphoned-off-in-2-days/articleshow/65399477.cms?from=mdr>, accessed April 2022.
12. Siponen, M. and Willison, R. Information Security Management Standards: Problems and Solutions. *Information & management*, vol. 46, no. 5, pp. 267-270. 2009.
13. www.gartner.com, accessed April 2022.
14. <https://appwiki.checkpoint.com/appwikisdb/public.htm>, accessed April 2022.
15. <https://www.fortiguard.com/encyclopedia/applications/>, accessed April 2022.
16. <https://applipedia.paloaltonetworks.com/>, accessed April 2022.
17. www.radware.com, accessed April 2022.
18. www.imperva.com, accessed April 2022.
19. Mishra, S. and Chasalow, L. Information Security Effectiveness: A Research Framework. *Issues in Information Systems*, vol. 12, no. 1, pp. 246-255. 2011.

S. Guru Prasad is a Research Scholar of the School of Management, Hindustan Institute of Technology & Science, Chennai, India. His research interests include Cyber Security & Strategy, Information Systems Management.

M.K. Badrinarayanan is a Professor of the School of Management at Hindustan Institute of Technology & Science, Chennai, India. His research interests include Entrepreneurship, MSMEs, Competitiveness, Strategy, Technopreneurship, Livelihoods, microfinance.

V. Ceronmani Sharmila is a Professor of the Department of Information Technology, School of Computing Sciences at Hindustan Institute of Technology & Science, Chennai, India. Her research interests include Computer Networks, Cyber Security, Cloud Security, Image processing & IoT.