International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Survey on: Practices in Indian Public Organizations implementing Cyber Security

Pratap M S,
PG Scholar,
Department of MCA,
Dayananda Sagar College of Engineering,
Bengaluru, Affiliated to VTU

Vibha M B,
Assistant Professor,
Department of MCA,
Dayananda Sagar College of Engineering,
Bengaluru, Affiliated to VTU

***Abstract*— Information and Data security is of high concern for almost all organizations. Intrusion though can be dealt with use of firewalls, better and much improved ways of detecting intrusions are through advanced software, but some non technical issues may also lead to unauthorized access, if ignored. This paper attempts to discuss these issues. A survey was conducted and responses regarding cyber security were collected. The survey aims to study the awareness of cyber security among public sector employees in India. The survey further aims to study different sources through which intrusion is taking place in present scenario.**

***Index Terms*— Data Security, Cyber Security, Hacking, Firewall.**

I. Introduction

If cyber security was easily addressed we wouldn't be writing this paper. The reality is that there are no easy or perfect answers to this challenge. Cyber security as an issue is too broad, there are too many devices being connected to the internet that have variable security, too many vulnerabilities in hardware and software, the rate of change in technology is too great, and actors with ill intent only need to be successful once while defenders of cyber security have to be successful all of the time.[2]

Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction. Cyber security can also be defined as the protection of systems, networks and data in cyberspace, is a critical issue for all businesses.

Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. With the growing volume and sophistication of cyber attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security. During a Senate hearing in March 2013, the nation's top intelligence officials warned that cyber attacks and digital spying are the top threat to national security, eclipsing terrorism.[3, 5-7]

In this paper we focus our attention on the governance, strategy, policies and procedures of public sector companies relating to cyber security.

The Internet is fast becoming a way of life for millions of people and also a way of living because of growing dependence and reliance of the mankind on these machines.[1] Internet has enabled the use of website communication, email and a lot of anytime anywhere IT solutions for the betterment of human kind. Internet, though offers great benefit to society, also present opportunities for crime using new and highly sophisticated technology tools. Today e-mail and websites have become the preferred means of communication. Organizations provide Internet access to their staff. By their very nature, they facilitate almost instant exchange and dissemination of data, images and variety of material. This includes not only educational and informative material but also information that might be undesirable or anti-social.[4]

Both the increase in the incidence of criminal activity and the possible emergence of new varieties of criminal activity pose challenges for legal systems, as well as for law enforcement.

Devices will become that attack vector of choice bringing in nastier threats and attacks, basic two-step verification will no longer be sufficient. The line dividing cyber and targeted attack will blur, as cyber criminals adopt methodologies more identified with targeted attack compaigns.[11]

Time and again there has been continued worsening of the threats we're familiar with today, as well as the early seeds of threats that can grow to the next level.[11]

Information security executives have always been faced with the problem of justifying security technology investments because the technology benefits are difficult to estimate.[12]

II. Cyber security scenario in India

In keeping with the general trend of growth of information technology worldwide, in India too there has been tremendous growth in use of information technology in all walks of life. The internet user base has increased to 100 million and total broadband subscriber base has increased to 12.69 million. The target for broadband connections by 2014 is 22 million. Today, India has 134 major ISPs, 10 million registered domain names (1 million '.in' domains) and over 260 data centers all over the country[8-9]. Significant increase in cyber space activities and access to internet use in the country has resulted in increased opportunities for technology related crime.

Lack of user end discipline and inadequate protection of computer systems allowing users to impersonate and cover their tracks of crime, has emboldened more number of users for criminal activities. As a result, today Indian cyber threat landscape, like other parts of the world, has seen a significant increase in spam & phishing activities, virus and worm infections[10]. The rate of computer infections and spam & phishing activities in the country keep fluctuating, making India figure among the active sources, as is generally seen in developed economies with high rate of IT usage.

III. Objective of the study

The authors are motivated to study the levels of improvement that could be attained over the current state of affairs of cyber security in India. Hence the ultimate objective of the study is to dwell into the current practices of Indian public sector companies and offer possible remedial measures.

IV. Sources of data

The data is directly collected from the concerned participants. We have selected participants from the Management Development Program conducted on Information intelligence and cyber security for the executives of public sector companies. The questionnaire is distributed to all the 75 executives of the program. Of the 75 executives only 60 responded to the survey. 56 responses are found to be complete in all respects and considered for the study.

V. Summary of Responses

The study concerns with cyber security in public sector companies where the practices are analyzed pragmatically. The study spans across six critical parameters viz, Education and awareness, privilege management, Removable media control, Monitoring activity, Malware protection and Network security. We discuss key trends and noteworthy items throughout, leaving others for the conclusions. We aren't passing judgment on the findings, however merely presenting them.

The survey response captured a diverse mix of companies. The questionnaire used for the study is shown in Table I below.

TABLE I. **Summary of positive responses to survey questions**

No.	Question	Responses and %	
	Education and Awareness		
1	Do you have a method of maintaining user awareness of cyber risks?	6	10.7%
2	Do you have relevant staff training program?	0	0%
	Privilege Management		
3	Do you have a strong password policy?	24	42.9%
4	Do you monitor user activity and control access to activity and audit logs?	4	7.1%
	Removable Media Controls		
5	Do you have a policy controlling removable media?	20	35.7%
6	Are all sensitive devices appropriately encrypted?	11	19.6%
7	Do you scan for malware before allowing connections to your systems?	18	32.1%
	Monitoring Activity		
8	Do you have a monitoring strategy?	14	25.0%
9	Do you analyze network logs in real time, looking for evidence of mounting attacks?	3	5.4%
10	Do you continuously scan for new technical vulnerabilities?	11	19.6%
	Malware protection		
11	Do you have an appropriate anti-malware policy and practices that are effective against likely threats?	18	32.1%
12	Do you continuously scan the network and attachments for malware?	2	3.6%
	Network Security		
13	Do you protect your network against internal and external attacks with firewall?	32	57.1%
14	Do you filter out unauthorized or malicious content?	12	21.4%

A critical examination of empirical data is presented below:

A. Education and Awareness.

This being one of the prominent area of cyber security it is first administered to the participants of this survey. The two questions in this category are concerned with the knowledge levels of the participants and the relevant training programmes arranged in the organization. In case of awareness of cyber risks 6 participants responded affirmative. This leads to only

11% of the professionals being aware of the prospective cyber risks. With reference to relevant staff training programmes no one responded positively, which exhibits that the training programmes in the organizations are very very poor.

The Figure 1 shown below clarifies the results.

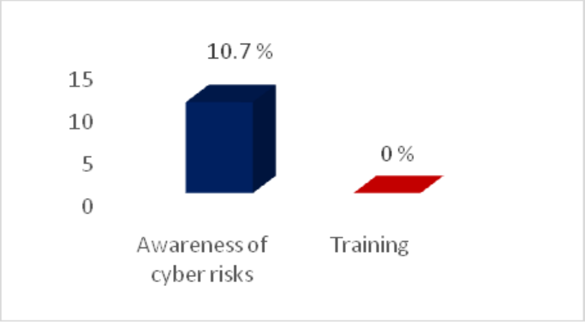

Fig. 1. **Survey respondents rating on Education and Awareness**

Overall the awareness levels and the necessary training are comparatively poor.

B. Privilege Management.

This is concerned with password policy and monitoring of user activity in the organization. As Figure 2 shows, 43% of respondents opined that they have a strong password policy, whereas only 7% agreed there is no monitoring of user activity and audit logs. This data exhibits that people are very much sensitive towards their password and its importance where as in case of monitoring and user activity and control access to activity and audit logs people are not that sensitive enough.

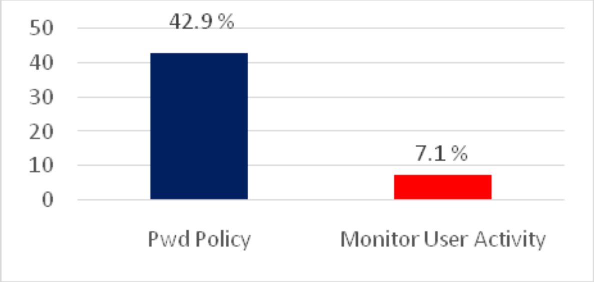

Fig. 2. **Respondents rating on Privilege Management**

C. Removable Media Control

This part of the questionnaire is concerned with the organizations policy of controlling access to external media devices and protection of sensitive devices through encryption. This section also enquires whether the participants scan for malware before connecting external devices to the network. In Figure 3, we see that about 36% of participants stated that they have a clear policy for controlling removable media, yet only about 20% of participants stated that sensitive devices are encrypted. 32% of respondents opined that they scan for malware and vulnerabilities before connections to the network are established.

This enables us to state that regarding the removable media controls and scanning for malware participants are aware of its benefits and difficulties to a better extent while in case of encrypting the device the participant's awareness levels are low.

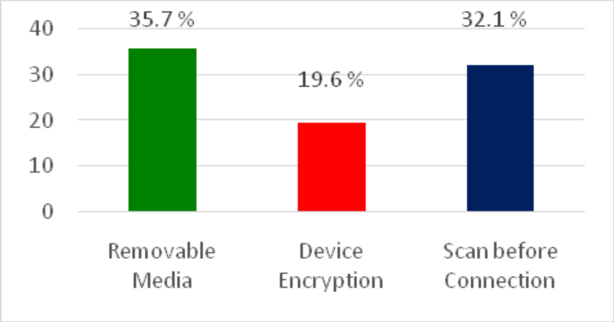

Fig. 3. **Respondents rating on Removable Media Control.**

D. Monitoring Activity

About 25% of participants stated that the organizations have a clear monitoring strategy (see figure 4). Only 5% of the respondents stated that they analyze network logs for evidence of attacks in the network, whereas 20% opined that they continuously scan the network for technical vulnerabilities. 14 out of 56 participants i.e., 25% stated that they have a clear strategy of monitoring vulnerabilities which is not a very encouraging number. Similarly 11 out of 56, i.e., 20% of the participants responded positively which is also not a very encouraging number with respect to scanning for new technical vulnerabilities. Still worse is the case of analyzing network logs for evidence of attacks where only 5.4% of participants are aware of.

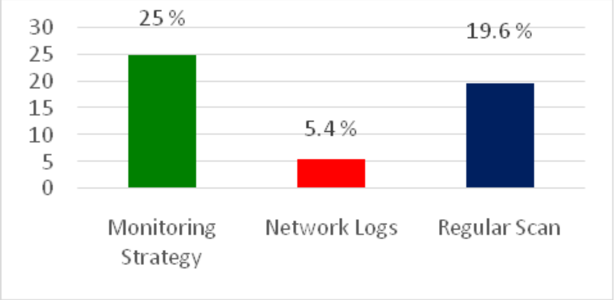

Fig. 4. **Respondents rating on Monitoring Activity.**

E. Malware Protection

Clearly, protection should involve regular scan of the network and the attachments, yet only a meager 4% of participants stated that they continuously scan the network and attachments for malware. As Figure 5 shows, 32% of the respondents have appropriate anti-malware policy and practices. Anti-malware policy is poor as 18 out of 56 i.e., 32% of the participants are aware of its discrepancies and difficulties. In case of scanning for malware in network and attachments the situation is pathetic as only 3.6% of the participants are aware of and practicing it.

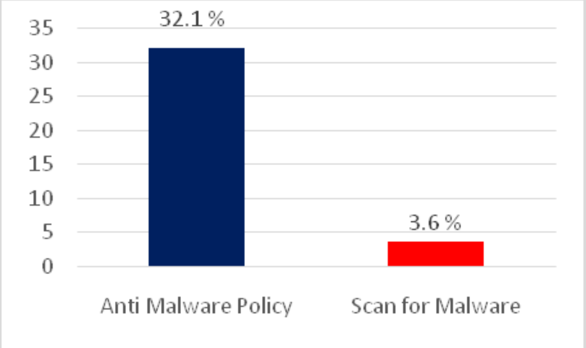

Fig. 5. **Respondents rating on Malware Protection**

F. Network Security

To prevent the information from being hacked, organizations use expensive hardware and software. Hacking could be easily avoided or could at least be reduced, if some precautions are taken such as protecting the network with firewalls. Among the respondents (see Figure 6), 57% stated that their network is protected with firewall against internal and external attacks, which is an encouraging number compared to others. About 21% of participants filter malicious and unauthorized content from the network; this is still a low number.

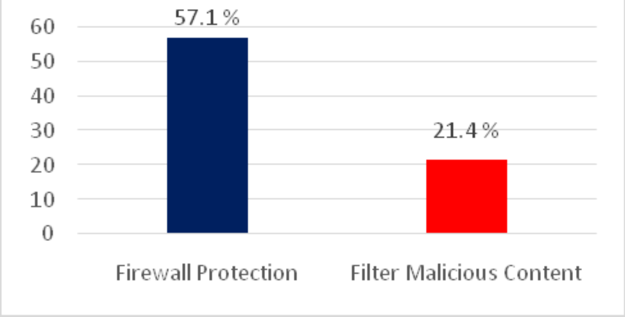

Fig. 6. **Respondents rating on Network Security.**

VI. Findings and Conclusions

A thorough analysis of participants responses to the six broad parameters i.e., education and awareness, privilege management, removable media control, monitoring activity, malware protection and network security spread across 14 questions is presented below. The fourteen questions studied show that participants are more knowledgeable and practice the safety measures with respect to protecting their network with firewall, strong password policy, control over removable media, scanning for malware using an anti malware policy. This enables us to conclude that participants are aware of only 5 of 14 parameters studied. This by any standards is poor. Even these above parameters are very much less than 50%. Regarding other 9 questions the participants knowledge are practices is very pathetic. Overall it can be concluded that the information security practices in the public sector companies in India is very deplorable and have to suggest a strong policy to employ suitable security measures to protect their data.

Organizations should begin at the core and direct their spending carefully. Make sure organization uses proper tools and protocols to protect the network. Proper employee education will also help mitigate risks associated with data breaches. Install and regularly patch security software to stay safe from attacks, especially those that rely on vulnerability exploitation.

Always remember that cybercriminals want to get their hands on your precious data. Take care when accessing your online accounts via any device, especially those that require revealing personal information.

IX. References

[1] Paul Rubens, “Anti-malware software can't spot all malicious code. Is isolating end-user tasks through virtualization a better approach to security?” May 30, 2014. http://www.esecurityplanet.com/open-source-security/are-anti-malwares-days-numbered.html.

[2] Adel Elmaghraby and Michael Losavio, Cyber Security in Smart Cities: Safety, Security and Privacy with the Internet of Things, Journal of Advanced Research (2014) 5, 413–414.

[3] “Comprehensive Study on Cybercrime.“ UNODC. Feb 2013. Q. 83. Web. 25 May 2014. http://www.amo.cz/editor/image/produkty1_soubory/the-impact-of-cyber-attacks-on-the-private-sector---briefing-paper.pdf.

[4] Vanson Bourne, “Protecting the Organization against the Unknown: A New Generation of Threats.”, Feb 2014. Web. 18 May 2014. http://software.dell.com/documents/protecting-the-organization-against-the-unknown-whitepaper-27396.pdf.

[5] Blitz, James. “Maude Warns on EU cyber security plans.” The Financial Times. 27 Mar 2013. Web. 2 Jun 2014. http://www.amo.cz/editor/image/produkty1_soubory/the-impact-of-cyber-attacks-on-the-private-sector---briefing-paper.pdf.

[6] “2013 Survey of Information Security Professionals: Defending Against State-Sponsored Attacks and Other Advanced Persistent Threats.” Lieberman Software. 4 Sep 2013. Web. 2 Jun 2014. http://www.amo.cz/editor/image/produkty1_soubory/the-impact-of-cyber-attacks-on-the-private-sector---briefing-paper.pdf.

[7] “The Economic Impact of Cybercrime and Cyber Espionage.” McAfee. 2013, p. 5.

[8] Rupinder Pal Kaur, Statistics of Cyber Crime In India: An Overview, International Journal Of Engineering And Computer Science ISSN: 2319-7242, Volume2 Issue 8 August.

[9] Dr. B. Muthukumaran, Cyber Crime Scenario in India, Criminal Investigation Department Review- January 2008.

[10] Ravikumar S. Patel, Dr.Dhaval Kathiriya, Evolution of Cybercrimes in India, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 4, July – August 2013, ISSN 2278-6856.

[11] Dhanya Thakkar, *Prediciting cyber hacktivists acts for 2014*, Information Week, Vol. 3, January 2014.

[12] F. Farahmand et al., "Assessing Damages of Information Security Incidents and Selecting Control Measures: A Case Study Approach," paper presented at 4th Ann. Workshop Economics of Information Security (WEIS 05), 2005.