

Advanced Cyber Security

by Robert Radu

Submission date: 11-Jul-2023 12:07PM (UTC+0100)

Submission ID: 210091275

File name: 30706_Robert_Radu_Advanced_Cyber_Security_507624_469546275.docx (51.31K)

Word count: 3414

Character count: 19937



Advanced Cyber security ACCB6000

Name: Robert-Mihaita Radu

Student Id:2029778

Assignment Title: Research, Implement, Analyse and Propose Viable Cybersecurity Strategies

Table of Contents

Introduction/Abstract: 3

Deliverable 1: Cyber risks and mitigation strategies: 3

Deliverable 2: Mitigation strategy from the Perspective of an Ethical Hacker: 9

Conclusion: 11

References: 13

Introduction/Abstract:

The aim of this paper to analyse the cyber risks of Lending Hands and provide mitigation strategies and recommendations for the organization. In the current interconnected world, ensuring the security of cyber space has been becoming an important priority. The main focus of this paper will be on Lending Hands which is actually a Ngo that is dedicated for helping vulnerable people globally. The NGO is facing several cyber risks so a suitable cyber security plan is needed for them. The main objective is to identify security flaws and vulnerabilities within the network infrastructure of the NGO, assess potential cyber threats, and propose a comprehensive mitigation strategy [1]. By analysing the technical security weaknesses and implementing specific recommendations, the NGO will be able to strengthen their cyber space and protect their physical and informational assets.

Deliverable 1: Cyber risks and mitigation strategies:

The increasing reliance of cyber security for several activities has made the cyber security a huge concern for the organisation. The NGO is facing various risks, the major risks identified for the organisation are:

Phishing attacks:

The phishing is actually a common type of cyber risks which is involved with malicious actors who send deceptive mails and messages for tricking the recipients in to forcing them to reveal sensitive information or downloading the malware. The employees of the NGO can be fallen in to this unknowingly to the phishing attempts where sensitive data and login details can be compromised.

Unauthorized access:

Weak passwords or insufficient access controls can lead to gain access by the hackers to the systems and network of NGO. It will result in the theft, alteration, or deletion of sensitive information, including fund sources, banking details, or beneficiary data.

Weak network security:

Weak network security measures like weak firewalls, unpatched systems, or misconfigured network devices, can leave the NGO vulnerable to the cyber attacks [2]. With the help of this, cyber attackers will be able to exploit the vulnerabilities for gaining unauthorized access, compromise data, or launch further attacks on the organization's network.

⁴ *Lack of incident response plan:*

Without a well defined incident response plan, the NGO might struggle to respond to as well as recover from the cyber security incidents, it can be the reason for long downtime of the system, increased damage and potential financial and reputational losses. There is also lack of security awareness and training for the employees which can increase the risk of falling victim to cyber threats [3]. Without proper training and awareness programs, the employees may also unknowingly engage in risky online behaviours or fail to recognize potential threats.

Third part risks and social engineering attacks:

The NGO can also rely on third party suppliers and vendors for several services or software. However, if these third parties have weak cybersecurity measures in place, they might become a vulnerable entry point for the hackers for gaining unauthorized access for the network of NGO or compromising their data.

For the organisation cyber security is so much important, as the organisation called Lending Hands, can handle huge amount of sensitive data including fund sources, beneficiary information, and financial details. The cyber security breaches can damage the organisational reputation severely, the new of security incident or security breach can also erode the trust among stakeholders including donors, beneficiaries, and partners [4]. Implementing robust cybersecurity measures demonstrates a ¹⁷ commitment to protecting sensitive information, fostering trust, and maintaining a positive reputation. The cyber security incidents can be having various financial implications for the cyber attacks, the costs those are associated with incident response, remediation, legal fees, and potential lawsuits can be substantial. In addition to that the organizations may incur financial losses due to stolen funds, fraudulent transactions, or the need to invest in recovery and rebuilding measures. For the organisation cyber security is an essential thing, so a suitable cyber security strategy is needed, the methods to resolve the situation along with the risks are:

1. **Strong password policies** – implementing powerful password policies which is crucial to secure against the unofficial access. Basically, the NGO should encourage the employees to utilize unique passwords and enforce the password complexity for multiple accounts [6]. Also, implementing multi-factor authentication can give additional layer of security by needing users to give extra verification like a one-time-code or a fingerprint.

2. **Employee awareness and training** – the NGO should implement a comprehensive cyber security awareness program to address the lack of employee training and awareness. Usually, this program should include daily training sessions on the cyber security best practices, password hygiene phishing awareness and data protection. Also, the training should be conducted to reinforce the importance of the cyber security and mandatory for every employee [5]. Implementing robust network security measures is crucial to secure against the data breaches and unofficial access. Basically, the NGO should consider implementing a firewall to control and monitor outgoing and incoming network traffic. However, utilizing a VPN for remote access can give a protected connection when the employees work outside the office premises.
- 1 3. **Regular software updates and patch management** – keeping systems and software up to date with the new security patches which is vital for preventing the vulnerabilities. Usually, the NGO should situate a patch management process to daily update the operating systems, firmware and applications across every devices. It is included with workstations, servers, mobile devices and laptops. 1 Evolving an incident response plan is important to minimize the impact of the cyber-security incidents [6]. Thus, the NGO should situate a step-by-step plan which outlines the actions to be taken in the event of a breach such as isolating affected systems, reporting the incident, notifying the appropriate authorities and conducting the forensic analysis.
- 9 4. **Data encryption and backup** – the sensitive and crucial data should be encrypted both at rest and in transit to mitigate the unofficial access. The NGO should implement the encryption protocols for the data transmission over the networks and make sure that the sensitive and crucial data is encrypted when gathered in the cloud or on the devices. The daily backups should be executed to mitigate data loss in the event to minimize the impact of cyber-security incidents. It is important to assess the security practices of these entities which is provided that the NGO shares its building with the other businesses. The NGO should implement the vendor risk management process to make sure that every business operating in the shared facility adhere to appropriate the cyber security measures.
5. **Employee privilege and access control** – implementing least privilege principles and proper access controls is vital to minimize the risk of unofficial access to crucial information. The NGO should daily update and review the user access rights that based

on the principle of least privilege, granting employees only the permissions to execute the job roles. Also, implementing a powerful IAM system can make sure appropriate permissions and assist the streamline access control processes which are assigned to the employees.

6. **Secure remote work** – provided the growing trend of remote work, the NGO should situate protocols and guidelines for protected remote work in the wake of the COVID-19 pandemic. It is included with using secure access solutions like the VPNs to secure the data transmitted into the network of the organization and the remote employees. The employees should also be boosted up to utilize the encrypted connections, educated on the risks that associated with the public Wi Fi network and protected the network protocols when working remotely.
7. **Regular security assessments and penetration testing** – the NGO should conduct the penetration testing and daily security assessments to proactively assess the effectiveness of existing security measures and find the vulnerabilities. Thus, these assessments can assist to find the potential weaknesses in the network, applications and systems and permit for timely remediation. Linking external cyber security professionals to execute the penetration testing which can give an unbiased evaluation of the NGO security posture [7]. Basically, the NGO should consider implementing security monitoring technologies and tools to respond and detect to the cyber security incidents in the timely manner. Thus, these can include IDPS, EDR systems and SIEM solutions. These tools can also assist to detect the potential threats, monitor network traffic and give real-time alerts for quick incident response.
8. **Continuous security training and awareness** – the cyber security attack vectors and threats develop quickly and making continuous awareness and training vital. Thus, the NGO should give ongoing cyber security training to employee to keep the users informed about the latest threats, mitigation strategies and attack techniques. Daily security awareness campaigns such as posters, email reminders and internal communications can assist to reinforce the value of the cyber security best practices among employees. Establishing a culture of the collaboration and security incident reporting within the organization is crucial. Basically, the employees should be boosted up to report any suspicious activities, security incidents and potential breaches. Also, the NGO should foster the information and collaboration sharing with the industry

groups, organizations and the government agencies to stay updated on the best practices and emerging threats.

The cyber security land scape can expose the organisations for the legal liabilities, specially if the sensitive information can be compromised or regulatory obligations are violated, by implementing the effective cyber security measures, the organisations will be able to minimize the risk of legal consequences and potential laws. The timeline to implement the cyber security measures for the organisation are:

Task Name	No. of Days	Start Date	End Date	Justification
Security Risk Assessment	5	20 Jul 23	24 Jul 23	Assess current security risks and vulnerabilities to identify areas of improvement.
Develop Cybersecurity Policy	7	25 Jul 23	31 Jul 23	Create a comprehensive policy outlining security guidelines, procedures, and responsibilities for all employees.
Employee Security Training	10	1 Aug 23	10 Aug 23	Educate employees on cybersecurity best practices, threat awareness, and their roles in maintaining a secure environment.
Network Infrastructure Audit	7	11 Aug 23	17 Aug 23	Assess the organization's network infrastructure for vulnerabilities, misconfigurations, and weak points.
Implement Firewall Solution	5	18 Aug 23	22 Aug 23	Deploy and configure a robust firewall solution to secure the

				network from unauthorized access.
Vulnerability Scanning	3	23 Aug 23	25 Aug 23	Perform automated scans to identify vulnerabilities in systems, applications, and network devices.
Penetration Testing	7	26 Aug 23	1 Sep 23	Conduct controlled simulated attacks to evaluate the effectiveness of existing security measures.
Wireless Network Security	4	2 Sep 23	5 Sep 23	Secure the wireless network by implementing strong encryption, access controls, and regular monitoring.
Laptop Security Measures	5	6 Sep 23	10 Sep 23	Enforce laptop security policies, including full disk encryption, strong passwords, and regular software updates.
Data Encryption	4	11 Sep 23	14 Sep 23	4 Encrypt sensitive data at rest and in transit to protect it from unauthorized access.
Incident Response Planning	7	15 Sep 23	21 Sep 23	13 Develop a detailed incident response plan outlining steps to be taken in the event of a cybersecurity incident.
Security Awareness Campaign	7	22 Sep 23	28 Sep 23	Launch an organization wide campaign to promote cybersecurity awareness and encourage a security conscious culture.

Implement Solution	SIEM	6	29 Sep 23	4 Oct 23	20 Deploy a Security Information and Event Management (SIEM) system for real time monitoring and threat detection.
Intrusion Detection/Prevention Systems		5	5 Oct 23	9 Oct 23	9 Install intrusion detection and prevention systems to monitor and block suspicious network activity.
Regular Audits	Security	Ongoing			Schedule periodic security audits to ensure ongoing compliance, identify new risks, and adapt security measures.

The organisation can also implement Security Information and Event Management (SIEM) for monitoring the network traffic, log events and detecting suspicious activities. It can help in timely identification as well as response to the potential threats. The organisation can also deploy intrusion detection/prevention systems for monitoring and blocking unauthorized access attempts along with malicious activities within the network.

Deliverable 2: Mitigation strategy from the Perspective of an Ethical

Hacker:

As an ethical hacker, the objective is identifying the security flaws with vulnerabilities within the Lending Hands network infrastructure, then according to the analysis of network specific recommendations will be proposed for strengthening the cyber security. The main aim will be aimed to help the NGO to understand their technical security weaknesses and providing actionable measures for protecting both informational and physical assets. For identifying the technical security weaknesses, the comprehensive assessment of the network infrastructure of the NGO should be conducted [8]. It will be included with performing regular vulnerability scans to identify known vulnerabilities in the network, servers, and applications. This will help in prioritizing patching and remediation efforts. Penetration testing will be also needed to be conducted for prioritizing patching and remediation efforts. The penetration testing will be

conducted for simulating the real world attacking scenarios and identifying potential entry points and vulnerabilities those are exploitable. It will help to uncover any kind of weaknesses which could be targeted by the malicious actors. The cyber security incidents can also expose the organisational activities to legal liabilities, especially if sensitive data is compromised or regulatory obligations are violated. By implementing effective cybersecurity measures, The NGO will be able to minimize the risk of legal consequences and potential lawsuits. The mitigation strategies which can be taken from the Perspective of an Ethical Hacker are:

1. **Network segmentation** – implementing network segmentation to limit the access to the sensitive details and restrict the lateral movement in the case of the breach. The NGO can control access and isolate the vital systems that based on the principles of least privilege by separating the network through the segments like the employee network, a guest network and server network [9]. Execute a thorough vulnerability assessment to find the potential weaknesses in the network infrastructure, applications and systems of the NGO. Thus, it can include scanning for known misconfigurations, vulnerabilities and outdated software versions. The assessment should also cover both external and internal systems to make sure the comprehensive view of the security posture of the network.
2. **Access control and authentication** – improve access control measures by implementing the powerful authentication mechanisms. Basically, it is included with enforcing the utilization of the complex passwords, daily reviewing user access privileges and implementing multi factor authentication. The NGO should also consider implementing PAM solutions to monitor and control the administrative access to the vital systems. Make sure that every system such as servers and laptops are configured with hardened settings [10]. Usually, it involves disabling unnecessary services, regularly patching and updating the firmware and software and applying the appropriate access controls. However, implementing the robust configuration management process can assist to prevent the risk of the exploitation of the vulnerabilities and the unofficial access.
3. **Employee security awareness** – improve employee security awareness into daily training campaigns and programs. The employees should be educated about common types of threats like social engineering and phishing and trained on the best practices for handling the crucial information. Regularity of security awareness campaigns such

as posters, email reminders and internal communications can assist to reinforce the value of the cyber security best practices among employees. By establishing a culture of the collaboration and security incident reporting within the organization is crucial. Basically, the employees should be boosted up to report any suspicious activities, security incidents and potential breaches. It also is included with emphasizing the value of verifying the email sender, reporting any security incidents promptly and avoiding suspicious attachments and links.

4. **Data encryption and privacy** – implement data encryption mechanisms both at the rest and in the transit to secure the important details from unofficial access. Usually, it is included with encrypting the data that gathered on the servers, laptops, etc. Adhering to the privacy regulations and data protection like the GDPR can gain the cyber security posture of the NGO.
5. **Regular penetration testing** – conduct the periodic penetration tests to find any new vulnerabilities which may have arisen and assess the effectiveness of the system. Therefore, this tests should give actionable recommendations and simulate the real world attack scenarios for strengthen the cyber security defences of the NGO. Update and evolve an incident response plan which outlines the steps to be taken in the event of the cyber security incident [11]. Usually, it is included with clear responsibilities and roles, a predefined process for mitigating and containing the impact of the incident and communication protocols.

By implementing the above recommendations the NGO will be able to enhance their security posture and protect both physical and informational assets. The regular assessment, incident response planning and training programs are so much crucial to maintain the strong cyber security stance [12]. As the ethical hacker, this is so much important to continue to monitor and update the security measures for staying ahead of emerging cyber threats and ensure that the NGO will be able to continue their mission of delivering transformational changes to the vulnerable populations globally.

¹ **Conclusion:**

Thus, it can be concluded from the report that for the NGO cyber security is a huge concern, so this is so much important to address their technical security weaknesses and enhancing the overall cyber security posture. The proposed strategy is included with an assessment of the

network infrastructure, identification of the vulnerabilities through penetration testing and vulnerability scanning and by security of the wireless network. By implementing the recommended security measures the NGO will be able to establish a strong cyber security framework, risk mitigation and enhancement of resilience against the potential cyber threats. By doing this the organisation will be able to navigate the cyberspace effectively and continue making transformational changes for improving the lives of vulnerable populations globally.

References:

- [1].A. S. Abdou, "Cyber Security and Privacy in Cloud Computing: Review," 2017 10th International Conference on Developments in eSystems Engineering (DeSE), Paris, France, 2017, pp. 137-142. doi: 10.1109/DeSE.2017.24
- [2].M. A. Hossain, M. A. Karim and A. Hasan, "A Comprehensive Study on Cyber Threat Intelligence," 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), York, United Kingdom, 2020, pp. 1-8. doi: 10.1109/CyberSecurity49315.2020.9138837
- [3].M. M. Hasan, M. Al Hasan, and K. Salah, "A survey on cyber security for smart grid communication networks," IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1986-1997, Fourth Quarter 2014. doi: 10.1109/COMST.2014.2326353
- [4].N. K. Meher and S. K. Rath, "A Comprehensive Study on Cyber Threat Intelligence," 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 2016, pp. 1984-1989. doi: 10.1109/RTEICT.2016.7808146
- [5].S. Gupta and B. Chakraborty, "Secure Data Storage and Retrieval in Cloud Computing: A Comprehensive Study," 2021 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), York, United Kingdom, 2021, pp. 1-7. doi: 10.1109/CyberSecurity51249.2021.9543079
- [6].S. Kumar, R. Kumar and R. Bhatia, "A Survey on Security Challenges in Software Defined Networking," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-6. doi: 10.1109/ICCCNT45670.2019.8944745
- [7].S. Kumari, V. Dey and A. Bhattacharya, "A Comprehensive Survey on Cyber Threat Intelligence Analysis Techniques," 2022 International Conference on Computing and Communication Systems (I3CS), Nagpur, India, 2022, pp. 1-6. doi: 10.1109/I3CS54430.2022.9607413
- [8].S. Mehnaz, A. Islam and M. A. Hossain, "Machine Learning Techniques for Detecting Advanced Persistent Threats in Cyber Security," 2017 6th International Conference on

Informatics, Electronics & Vision (ICIEV), Kitakyushu, Japan, 2017, pp. 1-5. doi: 10.1109/ICIEV.2017.8338321

- [9]. S. R. Challa and V. M. Reddy, "A Survey on Cyber Security Attacks and Defenses in Smart Grid," 2018 International Conference on Information Technology (ICIT), Bhubaneswar, India, 2018, pp. 1-6. doi: 10.1109/ICIT.2018.8473535
- [10]. S. Saini, S. Jain and S. S. Jadon, "Secure Communication in IoT Using Blockchain: A Review," 2018 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), Chennai, India, 2018, pp. 17-21. doi: 10.1109/ICSTM.2018.8747963
- [11]. S. Singh, M. Khambete and V. Deshmukh, "A Survey on Blockchain Technologies for Cyber Security," 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 2019, pp. 83-88. doi: 10.1109/SPIN.2019.8711569
- [12]. S. Zeadally, R. Hunt, Y. Baig, and A. A. Alelaiwi, "Cybersecurity for critical infrastructures: Attack and defense modeling," IEEE Communications Magazine, vol. 55, no. 3, pp. 78-85, March 2017. doi: 10.1109/MCOM.2017.1600253CM

Advanced Cyber Security

ORIGINALITY REPORT

12%

SIMILARITY INDEX

7%

INTERNET SOURCES

7%

PUBLICATIONS

10%

STUDENT PAPERS

PRIMARY SOURCES

1

Submitted to University of Wales, Lampeter

Student Paper

3%

2

Submitted to University of Westminster

Student Paper

1%

3

Submitted to University of Northumbria at Newcastle

Student Paper

1%

4

www.nu.edu

Internet Source

1%

5

faculty.pmu.edu.sa

Internet Source

1%

6

www.irjmets.com

Internet Source

1%

7

www.srmist.edu.in

Internet Source

1%

8

Submitted to CSU, San Diego State University

Student Paper

1%

9

Usman Ahmad Usmani, Ari Happonen, Junzo Watada. "Secure Integration of IoT-Enabled

1%

Sensors and Technologies: Engineering Applications for Humanitarian Impact", 2023
5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2023

Publication

10	kpfu.ru Internet Source	1 %
11	oa.upm.es Internet Source	<1 %
12	iiitdm.ac.in Internet Source	<1 %
13	Submitted to University of East London Student Paper	<1 %
14	infosec-conferences.com Internet Source	<1 %
15	Ganesh Chandrasekaran, Talakala Grace Hanusha, Shailendra Rajpoot, Rajesh Challa. "CAPT: A Context-Aware stateful Processing ecosystem for Telco infra management", IEEE Access, 2023 Publication	<1 %
16	www.isfcr.pes.edu Internet Source	<1 %
17	Submitted to WQE College Student Paper	<1 %

18

Adam Fadhli Bin Azeem Fazwan, Aisya Azhar, Nur Sofiah Binti Hanif. "Data Leakage on Social Networking Sites", Institute of Electrical and Electronics Engineers (IEEE), 2023

Publication

<1 %

19

Simon Tan, Kevin Fang, T. William Lester. "Post-pandemic travel patterns of remote tech workers", Transportation Research Interdisciplinary Perspectives, 2023

Publication

<1 %

20

smt.icconnect007.com

Internet Source

<1 %

21

Submitted to Universiti Putra Malaysia

Student Paper

<1 %

Exclude quotes Off

Exclude matches Off

Exclude bibliography Off