2022 ANNUAL RISK ASSESSMENT REPORT

ESecurity (Pvt) Ltd

ESecurity headquarters,
418 Galle Road, Colombo,
Sri-Lanka.

IT20208776 **- Madanayaka B.P.W (Leader)**
IT20215606 **- N.S.A Dias**
IT20134426 **- Samaranayake A.K.D.D.V**
IT20217204 **- Karawita K.V.D.A.U**

ABSTRACT

The primary goal of this risk assessment is to identify and possibly mitigate (if the risk level is high enough) weaknesses, vulnerabilities, and failures in the systems that ensure the flow of the Esecurity (Pvt) Ltd. Potential threats will also be evaluated, as well as their estimated financial impact on Esecurity. We will also discuss how these key issues have affected the company thus far, as well as recommendations for each issue that will help to mitigate these problems. For this assessment, we chose the Octave allegro risk assessment framework.

SCOPE

This risk assessment was performed by security governance team of esecurity company to identity risks and threats critical of the system.

1. EXECUTIVE SUMMARY

Perform an information security risk assessment on the ESecurity headquarters, 418 Galle Road, Colombo, Sri Lanka, between April 1, 2022, and April 25, 2021. The risk assessment is carried out and concluded when fundamental data is recognized.

This section outlines the significant issues identified by our team, which will be detailed in the technical report utilizing the well-known risk management framework "OCTAVE Allegro." We will also explain how these significant concerns have affected the company thus far, as well as recommendations for each issue that will help to mitigate these problems.

These three more important key factors are.

- An assessment of common and man-made threats.
- Predicted the nature and current state of reasonably expected cyber security controls.
- The overall creation of the IT protection program that focuses on the current abilities of individuals, processes, and technologies that are relied on to keep ESecurity HQ secure.

1.1 KEY ISSUES

- Issues in Network Failures.
- Issues in Customer Data disclosure.
- Backup for server downtime

1.2 RECOMMENDATIONS

- Data access policy can be implemented to ensure the data protection of the customer to avoid issues that are related to customer data access.
- A customer login monitoring system can be introduced to avoid customer identity theft.
- A third-party data non-disclosure agreement must be signed off to prevent the transfer of customer data to an unauthorized third party.
- Provide wide-ranging protections to prevent the impact of hurricanes, floods, and earthquakes.
- Assign a team to make sure the safety of the server.
- Check malfunctions on a regular basis and use high-quality equipment to ensure durability
- Encrypt sensitive data including customers' usernames and passwords.
- Full back up of applications including the private files stored on/data partition and customize this behavior by implementing a Backup Agent class.

2. DETAILED ANALYSIS

2.1 PURPOSE

The purpose of this evaluation is to safeguard against the vulnerabilities discovered in the first quarter of the year. Even a little defect becomes a major opportunity for attackers when used as a protective device. The present framework should be enhanced and updated with the most modern characteristics and software components to guard against cyber-attacks.

2.2 Why use Octave Allegro?

Our team chose Octave Allegro and conducted qualitative research based on the ESecurity structure. Octave Allegro was chosen for a variety of reasons.

- This will indicate all the risk factors which the system is exposed.
- Efficiency in terms of time.

2.3 APPROACH TO RISK APPRAISAL

2.3.1 PARTICIPANTS

ROLE	PARTICIPANT
System Owner	George Anthony
System Custodian	Robert De Silva
Security Administrator	Christian Almeidha
Database Administrator	Ishini Lansakara
Network Manager	Martin Wickramathunga
Risk Assessment Team	Bhathiya Madanayaka, Amaya Dias, Apoorva Karawita, Dihan Samaranayake

2.3.2 RISK APPRAISAL CRITERIA

We use a **qualitative risk analysis** and **quantitative risk analysis** approach when assessing risks associated with ESecurity.

2.3.2.1 QUALITATIVE RISK ANALYSIS

Risk = Probability * Magnitude of Impact

2.3.2.1.1 Magnitude of the Impact

Magnitude of the Impact	Description
High (100)	Loss of major assets, human resource harm, service contamination, financial losses, and contamination of a major objective are all examples of major assets losses.
Medium (50)	Loss of capital that can be managed, financial losses that can be tolerated, and a reduction in working capacity.
Low (10)	Properties are just slightly impacted.

2.3.2.1.2 Probability (Likelihood of occurrence)

Magnitude of the Impact	Description
High (1.0)	Immediate response/action is required
Medium (0.5)	Even though successful movement can be initiated, a moderate threat profile is present
Low (0.1)	Low system effect / the hazard has been managed by the system.

2.3.2.1.3 Risk Calculation

Threat Probability	Impact		
	Low	Medium	High
High (1.0)	1.0 X 10 = 10 LOW RISK	1.0 X 50 = 50 MEDIUM RISK	1.0 X 100 = 100 HIGH RISK
Medium (0.5)	0.5 X 10 = 5 LOW RISK	0.5 X 50 = 25 MEDIUM RISK	0.5 X 100 = 50 MEDIUM RISK
Low (0.1)	0.1 X 10 = 1 LOW RISK	0.1 X 50 = 5 LOW RISK	0.1 X 100 = 10 LOW RISK

2.3.2.2 QUANTITATIVE RISK ANALYSING

2.3.2.2.1 CRITICAL ASSETS

Critical Assets	Description	Container	Security Requirements	Value (LKR)
Administrative Server (AS)	Responsible for baking up administrative server data, Maintenance of the database, automatic distribution of reports	Dell PowerEdge R430 Tower Server with windows server 2012	**Confidentiality Integrity Availability**	Rs.9,800,000
Customer Information Database Server (CIDS)	All the information such as customer name, NIC number, Age, Residential Address, E-mail address and Banking Details are included in the Customer Information Database Server	Dell PowerEdge R430 Tower Server with windows server 2012	**Confidentiality Integrity Availability**	Rs.10,000,000
ESecurity Database Network (EDS) – Firewall	Firewall included to prevent the cyber-attack from the outside	Cisco software and hardware firewall	**Confidentiality Integrity Availability**	Rs.1,968,500
ESecurity Database Network (EDN) – Routers	An EDS receives and sends data on computer networks	TP-Link Routers	**Confidentiality Integrity Availability**	Rs.1,871,700
ESecurity Database Network (EDN) – Switches	EDS use to connect the client and servers and deliver the data reliably	Cisco Switches	**Confidentiality Integrity Availability**	Rs.1,477,640

2.3.2.2.2 THREAT ANALYSIS

<table>
<tr><th>Asset</th><th>Threat</th><th>Impact Assessment</th><th>Mitigation approach</th></tr>
<tr><td rowspan="4">Administrative Server (AS)</td><td rowspan="4">a) Internal Attacks from the employees</td><td rowspan="2">Server being down can impact an organization in many ways. In addition to the costs, the impacts like data lost, damage the image of the company(reputation) might also be caused.</td><td rowspan="4">Train On-Site Staff – To refrain from outages caused by human errors. Rs.50,000
Update procedures for maintenance- With new systems and infrastructure components being added all the time procedures for maintenance should be updated. Rs.50,000</td></tr>
<tr><td>Risk Level</td></tr>
<tr><td>Low | Medium | High</td></tr>
<tr><td>✓</td></tr>
<tr><td>Customer Information Database Server (CIDS)</td><td>a) Dos Attacks in CIDS.
b) Social Engineering attacks to obtain Customer Information.</td><td>CIDS server contains all the Customer Information including their banking details of they use mobile banking criteria. When considering these identified threats, it is identified that if these threats are exercised the Customer Data will be misused, lost or be corrupted.</td><td>• Install an intrusion Preventing system. Cost: Rs. 250,000
• Install patches for Vulnerabilities. Cost: Rs. 600,000
• Conduct Awareness sessions to educate</td></tr>
</table>

		Risk Level			the customer about Social Engineering and other types of attack vectors. **Cost: Rs. 20,000** • Implement a Cloud server and backup all original customer details to prevent any data manipulation. **Cost: Rs. 800,000**
		Low	Medium	High	
				✓	

Asset	Threat	Impact Assessment	Mitigation approach
ESecurity Database Network (EDS) - Firewall	**a) Misconfiguration the firewall** **b) DDOS attacks** **c) Lack of security patches** **d) A lack of deep packet inspection**	Attackers would have easy access to your network, which may do long-term harm to your company. Also, intruders can manipulate the whole the network of the organization **Risk Level** Low / Medium / High ✓ (High)	Network system auditing combined with alerting capability would provide you with the visibility and control you need. Auditing allows greater user transparency and lets you identify possible compliance incidents until they cause serious problems by allowing you to easily notice inappropriate interface modifications and clarify who changed what. **Cost: Rs. 500,000**
ESecurity Database Network (EDN) – Routers	**e) Unauthorized access** **f) Session hijacking** **g) Rerouting** **h) Masquerading**	• Loss of confidentiality • Loss of availability • Loss integrity **Risk Level** Low / Medium / High ✓ (Medium)	The first step in threat reduction is to disable all idle utilities that are running on the router. You may also reduce network risks by limiting the number of users and providers on the router. Since they serve as filters between the outside world and your network, ACLs are the most powerful. ACLs can also be used to develop and implement organizational security policies in your organization. **Cost: Rs.400,000**
EDN (Switches)	**i) Cam table attack** **j) ARP Attack** **k) Switch spoofing attack** **l) Man in middle.**	• Theft the credential of the system Corrupt the system. • Loss of confidentiality • Loss of availability • Loss integrity **Risk Level** Low / Medium / High ✓ (Medium)	Manually configure mac address. Implement the max number of MAC address. Disable the trunking on all access ports. Disable auto trunking and manually enable trunking. Configure IP address filtering. **Cost: Rs. 200,000**

3. Heat Map

1. **Administrative Server (AS)**
2. **Customer Information Database Server (CIDS)**
3. **ESecurity Android Mobile Application (EAMA)**
4. **ESecurity Database Firewall (EDF)**
5. **ESecurity Database Network (EDR) Routers**
6. **ESecurity Database Network (EDS) Switches**

IMPACT						
	100 - Catastrophic				3 - a	4 - b 4 - e
	Major			2 - a 2 - b		4 - a 4 - i 4 - c 4 - j
	50 - Moderate	1 – a 1 – b 1 – c		3 - b		4 - f 4 - k 4 - g 4 - l 4 - h
	Minor		2 - c 2 – d			4 - d
	10 - Insignificant	3 – c				
		Rare	Unlikely	Possible	Likely	Almost Certain
Probability		0.01		0.5		0.99

Low	Moderate	High	Extreme

4. TECHNICAL SUMMARY AND RECOMANDATIONS

The risk analysis process supports the effectiveness and efficient functioning of the organization by identifying the risks that require management attention. We have prioritized the identified risks involved in the ESecurity company according to the risk criteria presented in the beginning. As a best practice, eliminating the risk in the severity order is followed.

We believe security is not only a state but also the perception of safety. Information security, which is a specific element of an organization today, could be seen as both tangible and intangible. By considering the above asset replacements and by patching the vulnerabilities, your company can mitigate the vulnerabilities that can cause damage to your company. There are no 100% risk-proof scenarios in the real world.

There are many steps or actions to be taken as a result of the conclusion of the document. Some of them are,

- Get a cloud backup and recovery solution.
- Implement security software and appliances.
- Implement strict password and account management policies and practices.
- Implement firewalls, VPN, anti-spam, content filtering and other security layers.
- Bolster Access Control.
- Keep All Software Updated
- Use Network Protection Measures.
- checking the user's usual IP address or application usage patterns to avoid session hijacking.

REFERENCES

[1] Common Weaknedd Enumeration, "CWE-321 : Use of Hard-coded Cryptographic Key," Common Weaknesss Enumeration, 19 07 2006. [Online]. Available: https://cwe.mitre.org/data/definitions/321.html [Accessed 1 05 2021].

[2] MITRE Corparation, "CVE-2020-7962," The MITRE Corperation, 24 001 2020. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7962 [Accessed 01 05 2021].

[3] Android Developer, "Test backup and retore," Android, 27 12 2019. [Online]. Available: https://developer.android.com/guide/topics/data/testingbackup . [Accessed 01 05 2021].

[4] "geeks of geeks," geeks of geeks, [Online]. Available: https://www.geeksforgeeks.org/types-of-firewall-and-possible-attacks/.

[5] A. Pressley, "intelligentricio," intelligentricio, [Online]. Available: https://www.intelligentcio.com/eu/2017/10/16/the-5-most-common-router-attacks-on-a-network/.

[6] "compuquip cybersecurity," compuquip cybersecurity, 1980. [Online]. Available: https://www.compuquip.com/blog/firewall-threats-vulnerabilities

[7] Rhino Security Labs, "CVE-2020-5377 : Dell OpenManage Server Administrator File Read," 15 06 2020. [Online]. Available: https://rhinosecuritylabs.com/research/cve-2020-5377-dell-openmanage-server-administrator-file-read/. [Accessed 01 05 2020].

[8] "Imua," 24 September 1992. [Online].

[9] J. Douvinet, "Sciencedirect," Elsevier B.V., [Online]. Available: https://www.sciencedirect.com/topics/computer-science/network-failure .

[10] H. E. Mokadem, “Switch Attacks and Countermeasures”.