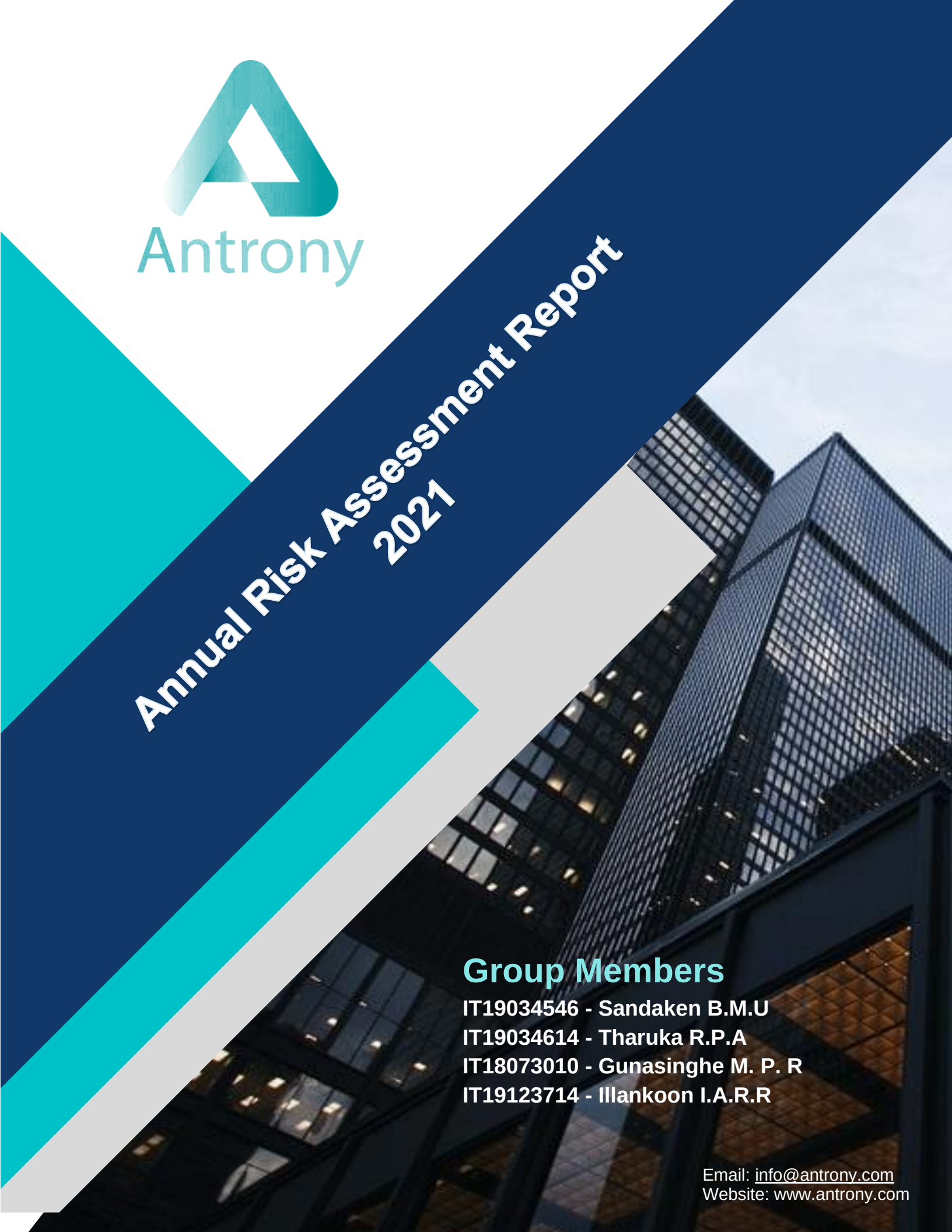
Antrony

Annual Risk Assessment Report 2021



Group Members

IT19034546 - Sandaken B.M.U
IT19034614 - Tharuka R.P.A
IT18073010 - Gunasinghe M. P. R
IT19123714 - Illankoon I.A.R.R

Email: info@antrony.com
Website: www.antrony.com

TABLE OF CONTENTS

1. Executive Summary

This security evaluation was carried out by Antrony Inc, Rochester, NY, on February 7th, 2020 to March 7th, 2020 which evaluates once in every year. The risk evaluation is carried out through the identification of critical information assets and potential threats to the security of information, such as confidentiality, integrity, and the availability of critical information resources.

Cyber-attacks can result in false assault warnings, critical communications or access to information can be interrupted, Intelligent sensitive information which includes weaponry planning or delivery systems can be compromised or even a rival can control the military defense weapons.

The risk assessment was carried out by Antrony Inc, risk management team using some additional analytical mechanisms mainly with the well-known OCTAVE Allegro framework.

2. Detailed Analysis

2.1 Introduction

Antrony Inc. is the Americas one of the exclusive providers of Military Defense weaponry. The business acumen of Antrony contains a wide scope of defense products. Warplanes, rotorcrafts, cybersecurity devices, surveillance suites, advanced weapons, missile defense. It works for the United States Air Force, the U.S. Army, the U.S. Navy, and several U.S. international allies. Antrony seeks to expand its frame to meet the demands of combatants and participate in next generation sequencing technologies to keep on top of future dangers also with journey of providing excellent, accurate, cost effective and timely armaments to the combatants globally.

Antrony workforce all around world are united by a shared vision to their value systems, that act as the core values for everything they are doing. Every one of them carries individual responsibility to implement and innovate in order to make the world better and to guide its teams, customers, stakeholders, and the communities they work in. They take responsibility for these values.

- For over 25 years Antrony has constructed and modified the Eagle weapon system.
- Today Antrony's missiles/Defense products are supported by more than 600 ships, 180 submarines, 12 different aircraft types, and Land-based launch vehicles.
- Antrony constructed over 25,000 small bombs in diameter

Since 1995 the military defense products including US Minuteman Intercontinental ballistic missiles (ICBM) have been developed and manufactured by Antrony. Today, Antrony has contracts for a wide variety of Defense products including Minuteman 3I missile work for over USD 200 million. It is anticipated that contracts will last until at least 2024.

2.2 Purpose

This risk evaluation driven for the discovery and analysis of vulnerabilities and threats in the various vital information assets of Antrony Inc.

2.3 Risk Assessment Framework

In compliance with the OCTAVE ALLEGRO framework, we decided to conduct this risk assessment, a well-defined information security risk assessment framework, giving greater consideration to risks related to company critical information assets.

Why this framework is chosen:

1. This methodology simplifies and optimizes the information security risk assessment process in order for an organization to achieve sufficient results through limited time, people, and other resources investment.
2. It fits perfectly with Antrony Inc, organizational structure.
3. Identify assets important for the organization's mission. Determine and assess the potential impacts of threats on the organization.
4. Have the ability to run vulnerability evaluation tools.

2.4 Antrony Inc, Team

Role	Member
Owner	Elizabeth Alexandra
CEO	Charles Philip Mountbatten
Security Administrator	William Arthur Philip
Database Administrator	Henry Charles
Security Management Team	James Bond, Kasim Maryia
Financial Planning Team	Peter John, Julian Sam

2.5 Risk Assessment Scope

Antrony is a renowned American supplier of Military Defense weaponry. Its services and products include military aircrafts, satellites, weapons and missiles, electronic military systems, launch systems and bombs. This risk assessment includes assets of information security such as confidentiality, availability of integrity. In this case, we also take into account customer trust, productivity, facilities, and safety requirements

Here we employed the OCTAVE Allegro Framework and this technical report's OCTAVE Allegro approach aims to allow a broad evaluation of the operational risk environment in an organization with the objective of producing stronger results without the need for extensive knowledge of risk assessment. This international standard is good for organizations that are intended to manage risks which could jeopardize information security of the organization. In addition, we discuss how critical assets are exposed to and mitigated by threats, vulnerabilities

2.6 Risk Model

2.6.1 Qualitative Analysis Parameters

Risk = Magnitude of Impact X Threat Probability

2.6.1.1 Magnitude of Impact

Impact	Score	Definition
HIGH	10	This has a significant effect. This can lead to significant asset and financial losses that are irreversible. It will either take proper handling or adaptation, or it will be impossible to handle.
MEDIUM	5	This has a major influence. This can result in the loss of recoverable assets as well as financial losses. In normal conditions, it is manageable.
LOW	1	This has a small impact. This can result in small financial and asset losses. It may be necessary to make an attempt to reduce management effort, or it may not be necessary.

2.6.1.2 Threat Probability

Threat	Score	Definition
HIGH	1.0	The threat source has a high chance of thwarting the scheme, and existing safeguards provide inadequate defense. Efficient countermeasures must be taken right away.
MEDIUM	0.5	The threat source has a moderate chance of thwarting the device, and existing safeguards have some defenses that could significantly mitigate the threat.
LOW	0.1	There is little risk that the threat source will be able to prevent the device, and existing protections provide near-complete defense.

2.6.1.3 Risk Calculation

Impact / Threat	Low (1)	Medium (5)	High (10)
High (1.0)	Low Risk (1.0 x 1 = 1)	Medium Risk (1.0 x 5 = 5)	High Risk (1.0 x 10 = 10)
Medium (0.5)	Low Risk (0.5 x 1 = 0.5)	Medium Risk (0.5x 5 = 2.5)	High Risk (0.5 x 10 = 5)
Low (0.1)	Low Risk (0.1 x 1 = 0.1)	Medium Risk (0.1 x 5 = 0.5)	High Risk (0.1 x 10 = 1)
Risk Scale: Low (0.1 to 1) Medium (>1 to 5) High (>5 to 10)			

2.7 Asset Profile

Critical Asset	Description	Security Requirements				Container	Value
		Property	H	M	L		
Experimental Weapons Information System (EWIS)	EWIS provides administrators with a web interface for convenient access to the framework and analysis of experimental outcomes. The experiments conducted for the weapons include preparing, assembling, tuning, testing and analysis.	Confidentiality	✓			HPE ProLiant ML350 Gen10 5218R 1P 32GB-R P408i-a 8SFF 2x800W RPS Server with Windows server 2016	$125,000
		Integrity	✓				
		Availability		✓			
Sensitive Information Systems (SIS)	SIS is used as Antrony's high-priority system that ensures the confidentiality of sensitive information in the company by protecting and managing all sensitive information.	Confidentiality	✓			HPE Superdome Flex 280 along with Microsoft Windows Server 2016	$20,000
		Integrity	✓				
		Availability		✓			
Access Control System (ACS)	ACS is essential a security measurement that is carried out within the Antrony's industries. Human access to the secured devices or facilities are managed, monitored, and regulated by ACS.	Confidentiality	✓			Cisco Secure Access Control System 5.7 with	$18,000
		Integrity		✓			
		Availability	✓				
Employee Management System (EMS)	EMS is a system that has all the personal and business-related details about the employees that work for the company	Confidentiality		✓		Dell PowerEdge R15 Rack Server with Citrix XenServer 7.1.0 CU2 Operating System	$15,000
		Integrity	✓				
		Availability		✓			
Sales Management System (SMS)	Antrony Inc's marketing and sales departments use the SMS to keep track of the selling process, which begins with the receipt of an order and ends with the sending of an invoice to the customer.	Confidentiality		✓		Intel Xeon E-2234, 32GB Memory, 8TB Hard Drive, H330 Controller with Windows Server 2019	$38,600
		Integrity	✓				
		Availability	✓				

H – High
M - Medium
L - Low

2.8 Threat Profile

Asset	Threat	Impact Assessment	Mitigation
Experimental Weapons Information System (EWIS)	**Threat:** Physical access to HPE Proliant Gen10 Servers with Intel Innovation Engine may result in the execution of unauthenticated Innovation Engine firmware, resulting in a local denial of service. **Vulnerability:** Windows Server firmware is outdated, and server is vulnerable to unauthorized code execution vulnerability and denial of service attack. (CVE-2020-8675)	Every experimental weapons information is highly sensitive and reliant on this EWIS. If a trespasser succeeds in carrying out an assault, the confidentiality of information would be violated, resulting in the disclosure of information to the public. This case would jeopardize the company's primary goals and result in a significant financial loss. Outcome: Destruction Risk level is **High**	Update HPE Server firmware to the new version Cost: $1000 Install Security information Manager Software. Cost: $2500 Annual Cost: $150

	Before Mitigation Applied	After Mitigation Applied
EF	68%	22%
SLE	$125,000 x 0.68 = $85,000	$125,000 x 0.22 = $27,500
ARO	0.67	0.67
ALE	$85,000 x 0.67 = $56,950	$27,500 x 0.67 = $18,425
Cost/Benefit	$56950 - $18,425 - $3,650 = + $34,875	

Asset	Threat	Impact Assessment	Mitigation
Sensitive Information Systems (SIS)	**Threat:** It could enable administrators to bypass security constraints and access multiple remote vulnerabilities such as disclosure of information or denial of service. **Vulnerability:** The current server is vulnerable to numerous remote vulnerabilities through incorrect administrator command input validation. Along with it, the OS is obsolete. (CVE-2019-11998)	Once a hacker could perhaps successfully, perpetrate the attack, the confidentiality of the data will be breached, ensuing in information being disclosed to the public. The cases damage the leading goals of the organization and provokes a massive financial damage to the company. Outcome: Disclosure, Modification Risk level is **High**	Update the Windows server version into 2019 and update the firmware. Cost: $1500 Annual Cost: $200

	Before Mitigation Applied	After Mitigation Applied
EF	54%	20%
SLE	$20,000 x 0.54 = $10,800	$20,000 x 0.20 = $4,000
ARO	0.40	0.40
ALE	$10,800 x 0.40 = $4,320	$4,000 x 0.40 = $1,600
Cost/Benefit	$4,320 - $1,600 - $1,700 = + $1,020	

Asset	Threat	Impact Assessment	Mitigation
Access Control System (ACS)	**Threat:** Since Active Directory is integrated with Cisco ACS, an attacker could potentially steal the domain administrator's credentials. **Vulnerability:** Inadequate validation of the Action Message Format (AND) protocol allows the existing ACS system vulnerable. An attacker will exploit this vulnerability by sending a modified AMF message which is carrying malicious code. (CVE-2015-0235)	Probability that unauthorized person accesses which leads to violation of confidentiality and integrity. In these situations, the organization experiences massive financial losses and Human lives are at risk as a result of the most dangerous occurrences. Outcome: Destruction Risk level is **High**	This vulnerability affects all Cisco Secure ACS versions prior to 5.8 Patch 7. Cisco has released software updates to fix this vulnerability. Enforcing new Intrusion Detection and Access Control. Example: VINDICATOR® V5 Cost: $700 Annual Cost: $100

	Before Mitigation Applied	After Mitigation Applied
EF	55%	20%
SLE	$18,000 x 0.55 = $9,900	$18,000 x 0.2 = $3,600
ARO	0.30	0.30
ALE	$9,900 x 0.30 = $2,970	$3,600 x 0.30 = $1,080
Cost/Benefit	$2,970 - $1,080 - $800 = + $1,090	

Asset	Threat	Impact Assessment	Mitigation
Employee Management System (EMS)	**Threat:** Attackers can exploit vulnerabilities in the system using traversal characters from which they can get access into the EMS's arbitrary files which contain all the employee information that are very sensitive. There are some instances where the attacker can write to arbitrary files which allows them to change the data or its behavior and eventually take full control over the system. **Vulnerability:** Path- traversal vulnerability, is a vulnerability that provides access to unauthorized users to read arbitrary files that are running in	If under any circumstance an attacker gets to access the system successfully, there could be total compromise to the system integrity by untheorized access allowing to completely shut down the system and hiding all the sensitive data in the system. Outcome: Modification, Disclosure Risk level is **High**	Update the Citrix XenServer version that patched the issue. Cost: $250 Install OSSEC Security Event Manager as an Intrusion prevention software. Cost: $1600 Annual Cost: $100

	the application. They can be either application code and data, credentials for the back-end systems, and sensitive operating files. (CVE-2018 - 14007)		

Before Mitigation Applied		After Mitigation Applied
EF	52%	15%
SLE	$15,000 x 0.52 = $7800	$15,000 x 0.15 = $2,250
ARO	0.67	0.67
ALE	$7,800 x 0.67 = $5,226	$2,250 x 0.67 = $1,507.50
Cost/Benefit	$5,226 - $1,507.5 - $1,950 = + $1,768.50	

Asset	Threat	Impact Assessment	Mitigation
Sales Management System (SMS)	**Threat:** The stock levels in the system are not completely managed by the system. The device will operate on the error values because it is unable to track down the errors caused by the employees. **Vulnerability:** Windows Server OS version is obsolete, and server is vulnerable to remote code execution vulnerability. (CVE-2019-1468)	The key goal of this framework was the monitoring of growth in revenue. If an employee makes an accidental mistake in stock levels, the company's financial situation will suffer, and fines will be imposed. It would, in the end, have an effect on the brand. Outcome: Interruption Risk level is **Medium**	Purchase stock managing software to collaborate with employees. Cost: $600 Annual Cost: $100

Before Mitigation Applied		After Mitigation Applied
EF	54%	20%
SLE	$38,600 x 0.54 = $20,844	$38,600 x 0.2 = $7,720
ARO	0.38	0.38
ALE	$28,444 x 0.38 = $7,920.72	$7,720x 0.38 = $2,933.60
Cost/Benefit	$7,920.72 - $2,933.60 - $700 = + $4,287.12	

3. Summary

Antrony Inc, Rochester, NY, conducted the Risk Assessment on February 7, 2020 through March 7, 2020, and reviews 17 systems that are known to Antrony once per year. Five critical systems have been identified by the 17-systems risk assessment team. The risk associated with selected 5 systems are described in this document. Antrony's 5 critical systems are the Experimental Weapons Information System **(EWIS)**, the Sensitive Information Systems **(SIS)**, the Access Control Systems **(ACS),** the Employee Management System (**EMS)** and the Sales Management System **(SMS).** We have identified a range of risks that might jeopardize their confidentiality, integrity, and availability. All threats associated to the systems and strategic plan for such systems have been outlined in the Threat Profile section. In addition, mitigation is included in the pre-mitigation and post-mitigation response plans and EF, SLE, ARO and ALE values.

For easy access to the framework and interpretation of experimental results EWIS offers a web interface for administrators. The upgrading of the HPE Server firmware to the new version is important as recommendations for current threats. In addition, the installation of the Security Information Manager software can reduce Antrony threats.

SIS is used as Antrony's high priority system to protect and manage the confidentiality of sensitive information within the company. This system also has an enormous impact as a high priority on the continuity of progress in the organization. For improved performance and security, we recommend updating the Windows server version to 2019 and updating the firmware.

ACS is a critical security measurement that is used in Antrony's industries. ACS manages, monitors, and regulates human access to secured devices or facilities. As a result, all three aspects of confidentiality, integrity, and availability need to be maintained. The team suggested that This vulnerability affects all versions of Cisco Secure ACS prior to 5.8 Patch 7. Cisco has issued software updates to address this vulnerability. Along with that, imposing a new Intrusion Detection and Access Control measures is a must.

The marketing and sales departments of Antrony Inc use SMS to track the selling process, which begins with the receipt of an order and ends with the delivery of an invoice to the customer. It is recommended that developers purchase stock management software for this system in order to collaborate with employees.

EMS is a system that contains all of the personal and business-related information about the company's employees. It is advised to update the Citrix Xen Server version that fixed the problem. Furthermore, installing OSSEC Security Event Manager as intrusion prevention software is required.

4. References

[1]S. Snyder and V. posts, "Boeing – Don't Bank on the Bomb", *Dontbankonthebomb.com*, 2021. [Online]. Available: https://www.dontbankonthebomb.com/boeing/#investments. [Accessed: 03- May- 2021].

[2]*Nsuworks.nova.edu*, 2021. [Online]. Available: https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=1191&context=gscis_etd. [Accessed: 03- May- 2021].

[3]"Boeing: Cybersecurity & Information Management", *Boeing.com*, 2021. [Online]. Available: https://www.boeing.com/defense/cybersecurity-information-management/. [Accessed: 03- May- 2021].

[4]"Dell EMC PowerEdge R815 - Citrix Hypervisor HCL", *Hcl.xenserver.org*, 2021. [Online]. Available: http://hcl.xenserver.org/servers/90/Dell_EMC_PowerEdge_R815. [Accessed: 05- May- 2021].

[5]"HPE Superdome Flex 280 Server | HPE Store US", *Buy.hpe.com*, 2021. [Online]. Available: https://buy.hpe.com/us/en/servers/mission-critical-x86-servers/superdome-flex-servers/superdome-flex-server/hpe-superdome-flex-280-server/p/1012865453. [Accessed: 05- May- 2021].

[6]H. Enterprise, *Support.hpe.com*, 2021. [Online]. Available: https://support.hpe.com/hpesc/public/home. [Accessed: 05- May- 2021].

[7]"PowerEdge T340 Secure Tower Server with iDRAC9 | Dell UK", *Dell*, 2021. [Online]. Available: https://www.dell.com/en-uk/work/shop/productdetailstxn/poweredge-t340. [Accessed: 06- May- 2021].

[8]H. Enterprise, "Document Display | HPE Support Center", *Support.hpe.com*, 2021. [Online]. Available: https://support.hpe.com/hpesc/public/docDisplay?docId=a00039149en_us&docLocale=en_US. [Accessed: 07- May- 2021].

[9]2021. [Online]. Available: https://buy.hpe.com/us/en/servers/tower-servers/proliant-ml300-servers/proliant-ml350-server/hpe-proliant-ml350-gen10-server/p/1010192786. [Accessed: 07- May- 2021].

[10]P. Support, C. System and C. Information, "Supported and Interoperable Devices and Software for Cisco Secure Access Control System 5.7", *Cisco*, 2021. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-7/device_support/sdt57.html. [Accessed: 07- May- 2021].

[11]Enterprise, H., 2021. *Document Display | HPE Support Center*. [online] Support.hpe.com. Available at: <https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=emr_na-hpesbhf04002en_us> [Accessed 7 May 2021].

[12]I. Process, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process", *Resources.sei.cmu.edu*, 2021. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419#:~:text=OCTAVE%20Allegro%20is%20a%20methodology,people%2C%20and%20other%20limited%20resources. [Accessed: 07- May- 2021].

[13]I. Process, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process", *Resources.sei.cmu.edu*, 2021. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419#:~:text=OCTAVE%20Allegro%20is%20a%20methodology,people%2C%20and%20other%20limited%20resources. [Accessed: 07- May- 2021].

[14]"Windows Server 2019 Compatible Servers", *Broadberry.com*, 2021. [Online]. Available: https://www.broadberry.com/server-os/windows-server-2019. [Accessed: 07- May- 2021].

[15]"Risk Heat Map", *CGMA*, 2021. [Online]. Available: https://www.cgma.org/resources/tools/essential-tools/risk-heat-maps.html. [Accessed: 07- May- 2021].

[16]Cve.mitre.org. 2021. *CVE -CVE-2020-8675*. [online] Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8675> [Accessed 7 May 2021].

[17]Cve.mitre.org. 2021. *CVE -CVE-2019-11998*. [online] Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11998> [Accessed 7 May 2021].

[18]Cve.mitre.org. 2021. *CVE -CVE-2015-0235*. [online] Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2015-0235> [Accessed 7 May 2021].

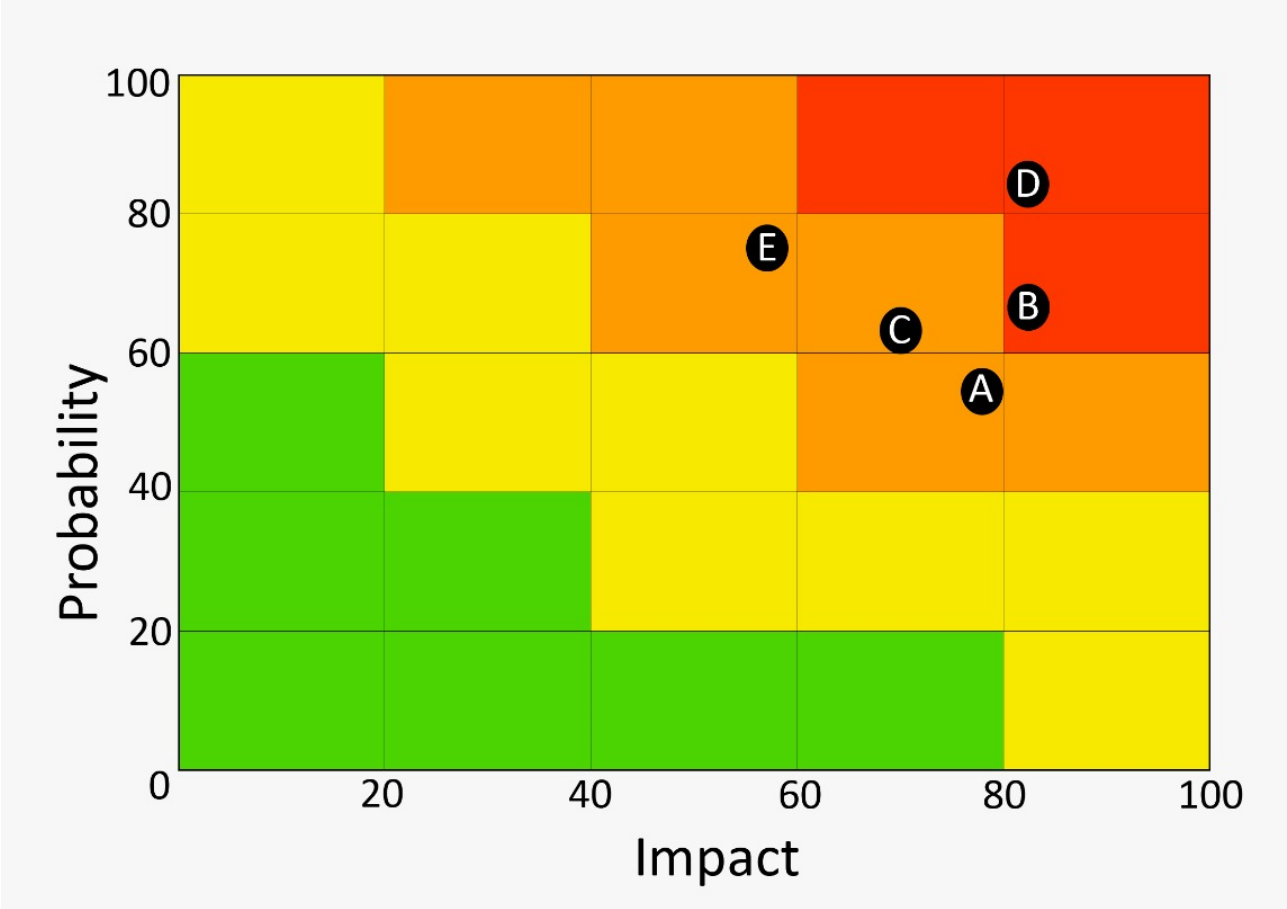
[19]Cve.mitre.org. 2021. *CVE -CVE-2019-11998*. [online] Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11998> [Accessed 7 May 2021].

[20]Cve.mitre.org. 2021. *CVE -CVE-2019-1468*. [online] Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1468> [Accessed 7 May 2021].

5. Appendices

5.1 Appendix A

5.1.1 Heat Map



A – Experimental Weapons Information System (EWIS)
B – Sensitive Information Systems (SIS)
C – Access Control System (ACS)
D – Employee Management System (EMS)
E – Sales Management System (SMS)

6. Appendix B

EWIS – Experimental Weapons Information System

SIS – Sensitive Information Systems

ACS – Access Control System

EMS – Employee Management System

SMS – Sales Management System

EF – Exposure Factor (Percentage of asset loss caused by)
SLE – Single Loss Expectancy (Asset Value x EF)
ARO – Annualized Rate of Occurrence (Frequency a threat will occur within a year)
ALE – Annualized Loss Expectancy (SLE x ARO)
Cost/Benefit – (ALE before Safeguard – ALE After Safeguard – Annual Cost of Safeguard)

6.1 SANS Guideline for Estimating the Potential Exposure Factor (EF)

1) Does attacked system has backup? Yes – subtract 15%

2) Is attacked system, behind firewall? Yes – subtract 10%

3) Is the attack from outside? Yes – subtract 8%

4) What is the rate of damage caused by attack? Subtract 3% if rate 25% damage/hour Subtract 18% if rate 5% damage/hour

5) What is the likelihood that attack goes undetected for in time of 100% recovery from attack? Subtract 3% if undetected for less than 20% of recovery time Subtract 15% if undetected for less than 10% of recovery time

6) How much time for implement countermeasures? Subtract 18% implement countermeasure less than ½ hour Subtract 10% implement countermeasure less than 1 hour Subtract 2% implement countermeasure less than 2 hour