Stark Inc.

STARK INDUSTRIES

RISK ANALYSIS REPORT 2022

PREPERED BY

Dilshan K.N(IT20021870)
P.A. Daham Thameera(IT20077624)
Wijesingha W.M.P.M(IT20023614)
Abeywickrama O.D(IT20153540)

Table of Contents

EXECUTIVE SUMMARY

This risk assessment was conducted on 'Stark Industries' constrained data innovation resources which was held on between March 30th and April 25th, 2022, and it was managed and performed by Stark Industries Management System's risk administration group to identify and present an outline of the threats affecting the data security properties, such as confidentiality, integrity, and availability, of a small number of simple systems. The three key rule components that direct "information risk," influencing the confidentiality, integrity, and availability of the chosen frameworks and data, are the focus of this hazard evaluation.

- An analysis of common and man-made threats
- The presence and performance of cyber security safeguards that are reasonably expected,
- The overall development of the IT security program, with a focus on the current capabilities of staff, operations, and cutting-edge technology that Stark Industries rely on.

KEY ISSUES AND RECOMMENDATIONS

- The Human Resource and Information Management System (HRIMS) must be updated.

The firmware of the 'Human Resource and Information Management System' server requires a patch update installation due to software and OS issues in the current state and firmware. On the other hand, the asset's value is optimal if a single clause is included in the organization's security approach guideline bimonthly updates.

- Complete replacements are required for Electrical and Telecommunication Management Systems (ETMS).

The server of ETMS is overheating due to physical vulnerabilities, such as the use of an ineffective power unit. To considerably reduce the harmfulness, a fresh new server cooling system must be purchased. Currently, the Uninterruptible Power Supply (UPS) pumping back up electricity is insufficient to keep the server running for the needed annual duration. A UPS that is currently in use must be replaced with one that has a higher capacity.

- A updated Financial Management System (FMS) is required.

The Financial Management System (FMS) wants to be updated to the newest version due to a software vulnerability in the expired FMS server. It also wants a separate backup strategy (Cloud storage) in case of an emergency.

- The hardware of the Resource Management System (RMS) requires a complete upgrade.

Due to a hardware flaw in the RMS server, it needs to have some hardware resources and performance upgrades.

- Irrigation Management System (IMS) automation with server connectivity is required.

Due to the obvious maintenance issues, the controlling procedure should be automated via server connections.

- The Military Management System (MMS) requires a full server update.

Due to Operating System software vulnerabilities in the MMS server router configuration's Access Control List (ACL), the server's OS and router configuration must be updated.

- Firewall management system (FMS) requires a full server update.
  A host header redirection vulnerability affects the remote host.

DETAILED ANALYSIS

SCOPE

Stark Industries is a multinational industrial company and the largest technical conglomerate in the world and the company founded in 1939 by Howard Stark [1]. The company is depicted as being owned and run by businessman Tony Stark, who is also known as Iron Man [1] According to Forbes 25's "Largest Fictional Companies" Stark Industries ranked as number 16.

The Stark Security Management System (SSMS) is the central structure that runs throughout Stark Industries' IT division. The SSMS refers to all of the essential, auxiliary, and tertiary systems and competences. It employs a variety of capacities and administrations to meet a variety of major and minor needs, including Security Services, asset and data management, budgetary administration framework, and so on. All residents and workers have controlled access to specific capacities and data advertised by and residing within the Stark Security Management System's subsystems, referred to as a ' SSMS'.

SSMS is so important to the organization that even a minor breakdown can throw the entire company and its dependents all across the north into disarray. SSMS is made up of more than ten information system resources that work together to provide the necessary data and functions for the organization's domain food. This system is built using a variety of servers in a variety of locations. The organization's estimate is comparatively 'medium,' with an estimated trade value about Rs. 2 billion.

PURPOSE

The purpose of this risk assessment was to examine and identify flaws and imperfections in various data innovation resources connected to the Stark Industries Management System, as well as to distinguish potential and/or current dangers associated with them and their estimated monetary impact on the organization. Furthermore, the risk assessment group will identify potential controls for the hazards, along with computed estimates for realistic mitigation, avoidance, transference, or acceptance plans. These estimations and cost/benefit analyses might next be examined by key organization individuals to decide on an ideal long-haul plan of action.

RISK ASSESSMENT FRAMEWORK

Having determined that the best way to do this risk assessment is to use the OCTAVE Allegro risk management framework. This system was chosen for a variety of reasons.

1. Restrictions and bounds that consider a variety of factors such as time, labor force, speculations, and so on.

2. This framework takes a 'Top to Bottom' approach, because of that it meets the needs of all specialized employees by making it easier to focus on each individual resource.

APPRAISAL RECEIVERS

Role	Organization Member	Signification
System Owner	Mr. Toney Stark	Owner
Director Board	Kalpa Haputhathri, Chethana Liyanage, Shenal Charles	Executive Member
Finance Manager	Nirmal Hewage	
Security Administrator	Nabil Jain	Technical Staff
Telecommunication and Systems Administrator	Sahan Sankalpa	
Database Administrator	Naveen Benjamin	

- **Functional**

  There are number of Critical asserts in the system. This risk assessment cover 6 main and critical system essential for the process.
- **Factorial**
  Appraisal includes data security qualities such as confidentiality, integrity, availability, accountability. to estimate the infringement on such components although contemplating the noteworthy elements such as wellness of the consumers, company reputation.
- **Personnel**
  By and large, 120-member evaluation collectors said over, IT division workers, common inhabitants, common representatives, and directors took an interest in the preparation of this chance appraisal. All these members are either inhabitants or representatives of the organization's domain.
- **Geographical**
  Server rooms, common IT office zones, and security guard rooms, to name just a few, were all guarded as part of the IT division.

Risk Management

Probability (Weight Factor)	In Detailed Information
High (1.0)	Vulnerability has been exploited by a risk source that is exceptionally knowledgeable and capable. The danger is either not covered by current controls, or the countermeasures supplied are ineffective in the face of a long-term hurdle to the risk. There is a pressing need for effective countermeasures that can be implemented immediately.
Medium (0.5)	The risk source has the capacity and willingness to take advantage of the vulnerability. Anti-exploitation procedures already in place are enough to prevent the vulnerabilities from being exploited again and over again. Risk is being under-appreciated a great deal.
Low (0.1)	The risk source, on the other hand, is unable to exploit the vulnerabilities effectively. Countermeasures and controls are seldom effective in preventing the danger from occurring.

Quantitative Analysis Parameters.

Risk = Threat Probability X Magnitude of Impact

THREAT PROBABILITY (SCALE)

Probability (Weight Factor)	In Detailed Information
High (1.0)	Vulnerability has been exploited by a risk source that is exceptionally knowledgeable and capable. The danger is either not covered by current controls, or the countermeasures supplied are ineffective in the face of a long-term hurdle to the risk. There is a pressing need for effective countermeasures that can be implemented immediately. [2]
Medium (0.5)	The risk source has the capacity and willingness to take advantage of the vulnerability. Anti-exploitation procedures already in place are enough to prevent the vulnerabilities from being exploited again and over again. Risk is being under-appreciated a great deal.
Low (0.1)	The risk source, on the other hand, is unable to exploit the vulnerabilities effectively. Countermeasures and controls are seldom effective in preventing the danger from occurring.

MAGNITUDE OF IMPACT

Impaction (Score)	In Detailed Information
High (10)	It is impossible for the organization to carry out its goal and trade if trade forms and/or important information are corrupted and/or misplaced. It is impossible for an organization's mission administration to continue when so many important aspects are changing. Workers' and clients' well-being and safety will suffer, and the company's budget will be impacted as a result. This will have an adverse effect on the company's reputation, customers, and revenue. (High) [2]
Medium (5)	Significant, however reasonable, obstacles to trade processes and/or critical information cause the effectiveness and efficiency of the operations to be of a substandard level where customers will be unsatisfied and disappointed. This will cause critical, however recoverable, budgetary and resource losses. (Medium) [2]
Low (1)	Negative effects on business operations and/or poor information led to modest decreases in productivity and efficiency, which disappoints customers. A little amount of money and resources may be wasted as a consequence of this. (Low) [2]

RISK WAS CALCULATED AS FOLLOWS

Impact / Threat Likelihood	**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 (0.5 x 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)]			

QUANTITATIVE ANALYSIS PARAMETERS

Variable	In detailed
Exposure Factor	Rate the degree to which a certain resource is exposed to a known risk circumstance.
Single Loss Expectancy	Exposure Factor (How much impact/loss to the resource may be predicted from a single risk occurrence) X Asset Value
Annualized Rate of Occurrence	The number of times a danger will occur in a calendar year. How likely is it that the chance circumstance will occur in a year? (Probability)

Annualized Loss Expectancy	Single Loss Expectancy X Annualized Rate of Occurrence (How much loss to the resource may be estimated over a year from the risk; this esteem indicates the risk)
Safeguard Cost	Annualized Loss Expectancy before Safeguard – Annualized Loss Expectancy after Safeguard – Safeguard Annual Cost

ASSETS PROFILES

A few basic stark industry are profiled here, with important details such as description, holder (where the data resources are prepared and stored), security requirements, and their values. (A-availability, I-integrity, C-confidentiality) [3]

Critical Assets	Description	Container and Specifications	Security Requirement
Human Resource and Information Management System (HRIMS)	This system stores and manages all information on employees in the industry, such as Work ID, Work Name, Leaving Details, Salary, Area of Expertise, and so on. This system is also in charge of all data and information. The most significant aspect of the entire system is the castle information system.	JBoss 4.2.2 (2) (Scan 3XS SER T25)	C – HIGH I – HIGH A –MEDIUM
Resource Management System (RMS)	The Great Lobby is home to Stark Industries, as well as a few keeps and towers that are used for various purposes at various times. As a result, the RMS is used to carry out the task of supervising their convenient assignments.	Fujitsu Primergy TX1310 M1 Server	C – MEDIUM I – HIGH A – HIGH
Financial Management System (FMS)	All information on goods in the kingdom that may be sold or spent by the people, such as stocks, budgetary resources, and so on. This system is used to store and monitor those items. Internal customers have restricted access to the framework's data and administrations via login credentials, however outside suppliers may also log in and view stock levels of certain items via the framework's internet interface.	Lenovo ThinkServer TS150 (Operating Windows Server 2012 R2)	C – HIGH I – HIGH A – MEDIUM
Military Management System (MMS)	The stark industry's security measures and management are based on a system. This is where you'll find all you need to know about the Stark Industry. Soldiers, weapons, military vehicles, existing models, testing models, quantity, capacity, function, and so on are all examples of this.	HPE ProLiant ML350 Gen 10	C – HIGH I – HIGH A – MEDIUM

Electrical and Telecommunication Management Systems (ETMS)	This system is built on power control frameworks, which include management, upgrading, and supplying, among other things. The majority of the communication controls revolve around server-based satellite connection management.	Dell PowerEdge T30	C – HIGH I – HIGH A – MEDIUM
Irrigation Management System (IMS)	This tire is in charge of the industry's irrigation system.	HP Proliant Microserver Gen8	C – LOW I – LOW A – MEDIUM

THREAT PROFILES AND MITIGATION ANALYSIS

Current or potential threats are profiled for the previously identified assets, using existing vulnerabilities, while establishing their qualitative effect and measuring their quantitative impact both before and after the suggested mitigation. [3] [4]

Critical Assert	Vulnerabilities	Threat Profile	Impact Assessment	Mitigation Plan	Cost / Benefits
Human Resource and Information Management System (HRIMS) (JBoss 4.2)	HRIMS's activities are carried out using a JBoss web servers. Version 4.2 is out of date. Updates are infrequent.	JBoss Enterprise Software Platform (aka JBoss EAP or JBEAP) 4.2 prior to 4.2.0.CP08 and 4.3 prior to 4.3.0.CP07 send the JMX password and other command-line parameters to the twiddle.log file, allowing local users to get sensitive information by reading this file.	Completely breach confidentiality. Allows for illegal information leak and service interruption.	JBoss should be updated to a newer version.	27,000
Resource Management System (RMS) Hardware	To hold more data, the RMS server requires greater storage capacity. And the system has to be updated because it is out of date.	Because of the increased resources and the obsolete OS of the present server, it must be updated, and new storage devices installed.	Violate Availability,	Install new data storage and upgrade the operating system.	520,000

Irrigation Management System (IMS)	The opening and shutting of sluice gates must be automated.	IMS must be automated due to a lack of manpower and knowledge.	Violate Availability	Purchase a high-quality automated software system.	77,000
Financial Management System (FMS) Backup System	FMS does not have a backup plan. Furthermore, the programmed is out of date.	FMS must do regular cloud backups because to ransomware.	Financial Service availability, integrity, and secrecy are violated.	Installing a cloud storage service and updating the system	170,000
Electrical and Telecommun-ication Management Systems (ETMS) Cooling, UPS and Devices	ETMS Server overheated as a result of the recent system downtime. The current UPS is unable to provide the necessary power to the system.	ETMS server overheating due to a lack of ventilation. Because of the limited capacity of the UPS, it cannot provide the power that the system requires.	Violate Availability, Integrity	Purchase a large capacity UPS and install a new air flow system.	1,500,000
Firewall management system(FMS) (FortiGate 5.2.15)	A host header redirection vulnerability affects the remote host.	The remote host is running a version of FortiOS older than 5.2.15 or 5.4.0 older than 6.0.5. As a result, it is vulnerable to a host header redirection vulnerability in the SSL VPN web interface as a result of a failure to correctly validate HTTP request headers [5, 3].	An unauthenticated, remote attacker can take advantage of this by redirecting SSL VPN web portal users to arbitrary web sites via a specially crafted HTTP request.	Upgrade to 5.2.15, 6.0.5, or 6.2.0 or later version of Fortinet FortiOS. Alternatively, use one of the workarounds described in the linked advice.	67,000

SUMMARY

We strongly recommend adopting an Enterprise application platform as an application server because the current jBoss server has a high failure rate owing to its free and outdated nature. Because of the problems associated with ransomware, the Financial Management System requires cloud storage for backup. FortiGate Firewall management system also have vulnerability in the current version. So, it needs to be update according to bug fixed version. The Resource Management System necessitates more storage space as well as system upgrades. Safe Access Control List setup is required for Military Management System routers, and Windows 2008 Servers should be updated to Windows 2012 Servers. Due to an overheating problem on the Electrical and Telecommunication Management System, a systematic cooling system must be constructed as soon as possible, and a big capacity UPS with a minimum capacity of 2000W is necessary. Irrigation management systems necessitate the use of a properly automated software system.

It is critical that these solutions be implemented in the system within the next month. Aside from purchasing equipment and software, Castle staff should be educated on fundamental computer dangers and vulnerabilities, as well as how to prevent them and use the resources responsibly. We recommend a security awareness training for personnel with varying levels of access to the system. This will lessen the threat of unintended assaults caused by a lack of information. We propose that the firm maintain comprehensive documentation for system maintenance. This will be important in identifying significant issues if a problem arises in the future.

Reference

[1] M. univers. [Online]. Available: https://marvelcinematicuniverse.fandom.com/wiki/Stark_Industries.

[2] J. S. A.Fakhrozib, "Assessment of Information System Risk Management with Octave Allegro at Education Institution," Procedia Computer Science.

[3] B. s. b. s. o. 2. |. TechRadar.. [Online]. Available: https://www.techradar.com/news/best-small-business-servers (.

[4] U. O. Structures., "Understanding Organizational Structures.," [Online]. Available: https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/understandingorganizationalstructures.aspx.

[5] Tenable, "Fortinet FortiOS < 5.2.15, 5.4.0 < 6.0.5 SSL VPN web portal Host Header Redirection (FG-IR-19-002)," Tenable, 29 04 2021. [Online]. Available: https://www.tenable.com/plugins/nessus/125889. [Accessed 04 2022].

[6] Wikipedia. [Online]. Available: https://en.m.wikipedia.org/wiki/Stark_Industries.