**DeepRock Gaming Inc. Strategic Cybersecurity Plan**

**Minh Ly**

**Favier Hu**

**University of Dallas**

CYBS 8396 – Strategic Cybersecurity Practicum

Spring 2021

Dr. Sandra Blanke



**Table of Contents**

Introduction (business name, industry and industry)..................................................... 3

Business Mission & Vision & Values............................................................................. 4

Strategic Security Goals….......................................................................................... 6

Strategic Security Goals Justification........................................................................... 5

IT Philosophy........................................................................................................... 9

Organization Chart and Reporting Structure............................................................... 11

Security Organization Description............................................................................. 13

Security Organization Justification................................................................... 14

Security Mission Statement............................................................................ 15

Security Core Values..................................................................................... 16

Security Issues and Challenges................................................................................. 19

Conclusion............................................................................................................. 21

**Introduction:**

DeepRock Gaming Incorporated is a pioneer in the social-network gaming industry that facilitates a connected environment for developing video games that appeal to people of all ages and genders and a platform for each of our players to connect with each other across all of our games. We currently lead the gaming industry with $8 billion in revenues in 2020 and $800 billion in operated holdings as of quarter one in 2021.

Through the first 15 years of our company, our organization has put an emphasis on allowing the ideas of our developers to be communicated with each other both easily and freely. This led to the development of our own platform and network that would provide both our employees and customers with the necessary tools to collaborate with each other in both an efficient and effective manner. As a result of our efforts, we have witnessed several moments of success in our company with our developers going on to create AAA title games that eventually became household names across the globe.

As DeepRock persists in placing the quality of communication between our employees and customers at an elevated level, another one of our objectives is ensuring that our platform for communication is both safe and secure. Our method behind securing our platform is primarily built on the principle that DeepRock can obtain key cybersecurity insights embedded within company structures and employ effective approaches to identify, detect, and isolate cybersecurity risks. We maintain company leadership through meeting cyber-risk management policy goals and meet and overcome key hurdles in all cyber environments.

Moreover, as a global establishment, we competently employ the gains of incessantly constructing regional and international relations to provide essential services that permit our establishment to oversee customer’s security properties across the world. This has granted us the freedom DeepRock requires to continue our pledge to concentrate on clients who have strong ties of investments to our company.

In DeepRock, we recognize the importance of safeguarding both the data of our company and the data of our customers. Therefore, we retain the confidentiality and safety measures of such information by utilizing the innovative technical cybersecurity controls we use to defend this data along with industry safety standards, and a robust philosophy of pre-established policies as stated in our policy reports affiliated with DeepRock’s professional foundations.

Sincerely,

*Hildenberg Preslin*

Chairman & Chief Executive Officer.

# **Business Mission, Vision, and Values**

**Mission:**

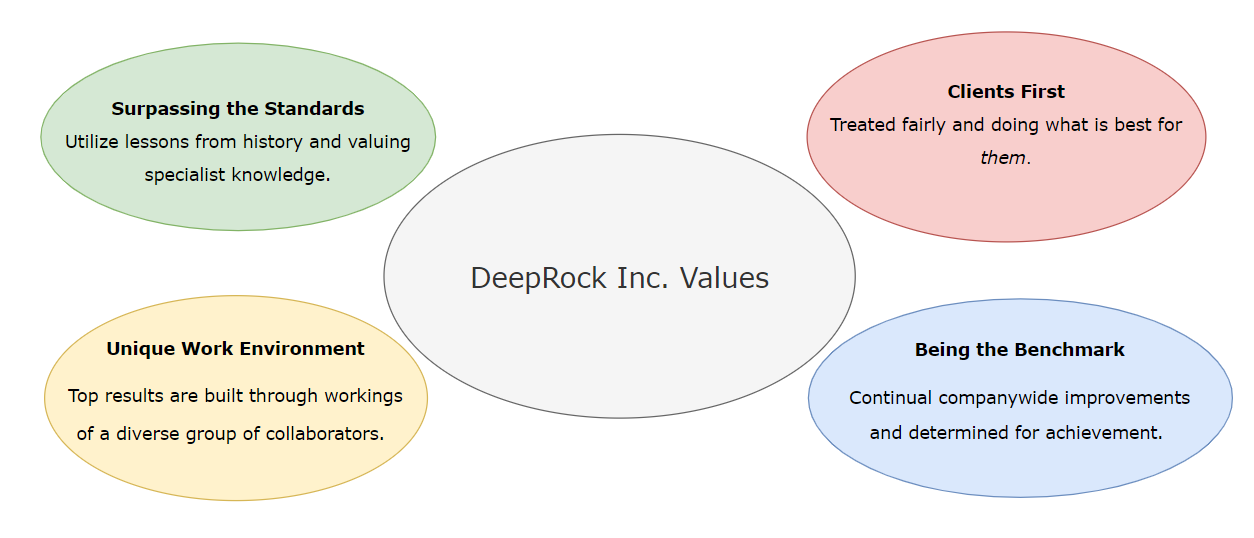
DeepRock’s mission is to create high quality entertainment for our customers, provide a safe and secure method of connection and communication for both our employees and our customers, and protect the confidential information of our customers.

**Vision:**

Our vision is to be the leaders in the social-network gaming industry with our players being connected all around the world no matter what game they are playing. In doing so, we will build a bond between our company and its users that reaches far past the standard.

**Values:**

DeepRock’s values originate from the key elements depicted in the diagram below.

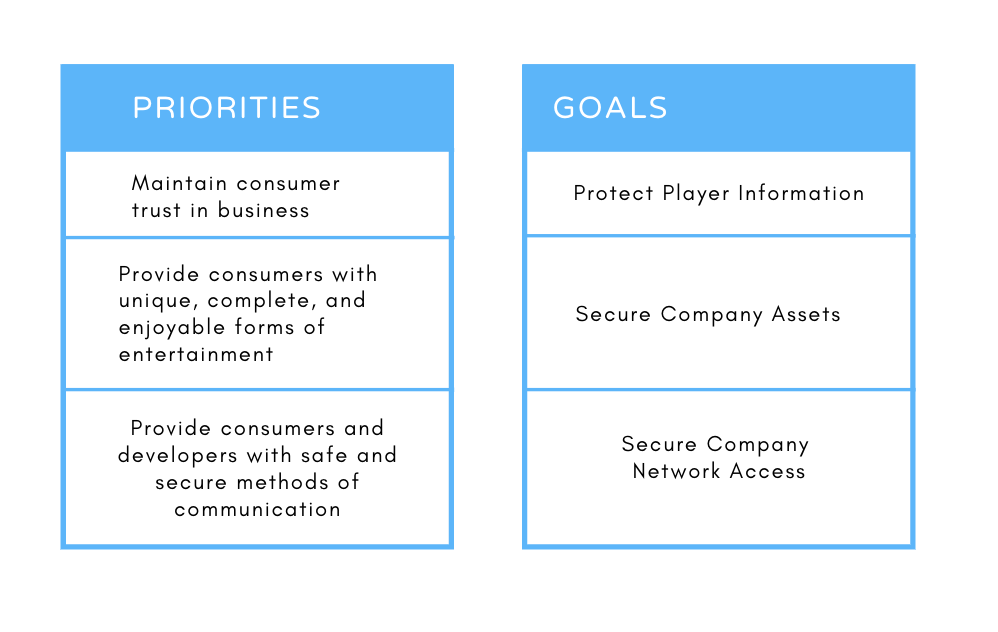


**Strategic Security Goals**

Security Goals Outline

| **Goal #1: Protect Player Information** |
| --- |
| Objective 1: Ensure player information stored on our servers is properly encrypted. |
| Objective 2: Systems and networks are to be programmed with self-defense tools with the use of active detection and response to threats and vulnerabilities regarding player information. |
| Objective 3: Implement systems for continuous maintenance of tools for security updates and patches. |
| **Goal #2: Secure Company Assets** |
| Objective 1: Implement full-disk encryption across all employee work devices |
| Objective 2: Facilitate enhanced cybersecurity resources |
| Objective 3: Grow a workforce that is aware of Cybersecurity needs |
| **Goal #3: Secure Company Network Access** |
| Objective 1: Implement security awareness training and testing program for employees who are working remotely. |
| Objective 2: Implement guidelines on proper device and router setup for remote employee workstations. |
| Objective 3: Acquire a trusted third-party VPN service. |
| Objective 4: Ensure proper segmentation of the network is applied. |

Business/IT Priority Alignments



**Strategic Security Goals Justification**

Goal #1: Protect Player Information

One of the most important aspects of DeepRock Gaming’s dealings with the online gaming industry is the need to protect the information of a consumer in matters regarding transactions or account logins, such as names, emails, addresses, or credit card information. Along with these, DeepRock must also be able to ensure that the data generated by players across all of our games is safely stored on our servers in order to prevent modification of data in a way that may give certain players an unfair advantage over other players. Failing to protect the critical information of our customers will result in severe consequences for both our customers and the integrity of our company. Thus, we have decided to set our most important goal towards working on this issue. In achieving this goal, DeepRock will be able to not only successfully keep our players satisfied, but keep the trust of our playerbase as well.

In order to achieve our goal of protecting the critical information of our customers, the first objective that we believe we must deal with is making sure their information is properly encrypted when stored on our servers. This would require research into which encryption methods are both efficient and effective for our purposes as well as setting up a system for proper management of encryption keys. The next objective would be to then put resources into acquiring both antivirus software and intrusion prevention systems for preventing and detecting harmful software or attacks. Furthermore, many hacks into systems occur due to failure to update these kinds of tools with the latest patches. In order to prevent attackers from exploiting known security holes, systems will have to be set up for maintaining these tools to ensure they are always up to date.

Goal #2: Secure Company Assets

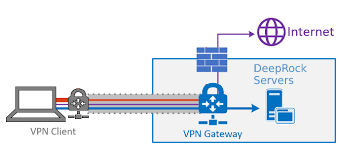
Information technology is rapidly evolving around the world to account for the needs of companies and their ongoing defense from outside threats trying to hinder them. Here at DeepRock Gaming, many of our assets come with the development of our exclusive games found on our company game client DeepRock Entertainment. However, a large portion of our assets are also found in our users who sign up and create their accounts on our client providing us their information when buying our games and modifying their own personalized profile for others in our community to see. We have a large social media presence in the gaming industry and are quickly growing in overseas markets creating a wide web of users all around the world meeting one another with a mutual connection of gaming. While this has primarily been touched on in Goal #1 of our report, we need to keep our large community of gamers in mind when developing security for our overall company assets. The source code for our games is imperative to our daily functions and uniqueness amongst the large ocean of gaming companies, so we must properly secure all of our game developing assets for our users and keep them satisfied with our products.

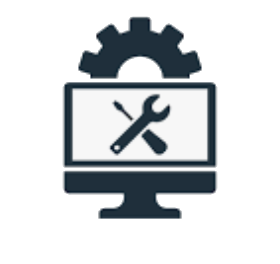
We at DeepRock Gaming are adamant on doing everything in our power to provide well-developed and *complete* products to our users. We cherish our users and promise to keep an edge over our enemies' demands. We strive to implement new mechanisms to deliver innovative cyber security capabilities and become more responsive to any breaches of important data found in our source code or developer’s information. Agility in policies, support, and procedures plays a large part in having a competitive advantage in the gaming industry when dealing with malicious individuals. Just as in any business, there will always be moving parts with data found in the company, many individuals in the gaming industry wish to find any bit of information in our source code to either trade in the black market or even sell to competitors in the industry. It is an essential goal for every process in our security department to have continuous improvement mandated. So many gaming companies have fallen victim to malicious hackers attacking them when their guard is down or more recently after they have been hit with backlash after a product of theirs was not up to standard with what the gaming community wanted. By moving forward with highlighting ideas and the implementation of notions to facilitate continuous planning, modeling, and performance of our responses to the outside environment seems only ideal for our gaming company. The focus of our goal to protect our company’s assets does not only focus on us, however, it incorporates so many other factors along the way, fostering innovation. These new ideas inherently change the overall cybersecurity system at DeepRock. For us to protect what we hold as our heart (source code), we must improve our ability to control processes to create, test and implement new ideas which influence the acquisition procedures to advance our overall cybersecurity mission at DeepRock.

DeepRock must reinforce the utilization of awareness programs that will educate employees about certain if not all types of intellectual property assets that must be secured. An awareness program being provided to each existing or new employee can be truly effective for preventing any asset leaks, however, only if it is targeted to the information that a specific group of employees needs to guard. Workers in any department at DeepRock, especially the IT department, should know the gravity at which he/she is making their decisions in regard to giving permissions to confidential company information to anyone. When one speaks in specific terms about something that engineers have invested a lot of time in, they are attentive. Humans are regularly a weak link in the defensive chain. That is why while a company may have protection that relies entirely on firewalls, but does not focus on employee awareness is destined to fail. In many cases, gaming studios assets leave an organization by accident or through *negligence*, so it cannot be stressed anymore to make sure employees are aware of how they might unintentionally endanger company assets.

Goal #3: Secure Company Network Access

Another critical factor of DeepRock’s business is the social aspect and our focus on communication and collaboration. As a result, we found it imperative to take measures towards protecting the infrastructure of our network from unauthorized access or disclosure. Doing so provides our developers with the security that they need in order to exchange their ideas without the worry of having those ideas being stolen or sabotaged. Furthermore, DeepRock’s network is utilized not only by our own organization for collaboration between our developers, but by our customers as well through our social-networking platform. Our customers must be able to reliably communicate with each other, meaning we must secure our network to satisfy our customers as well.



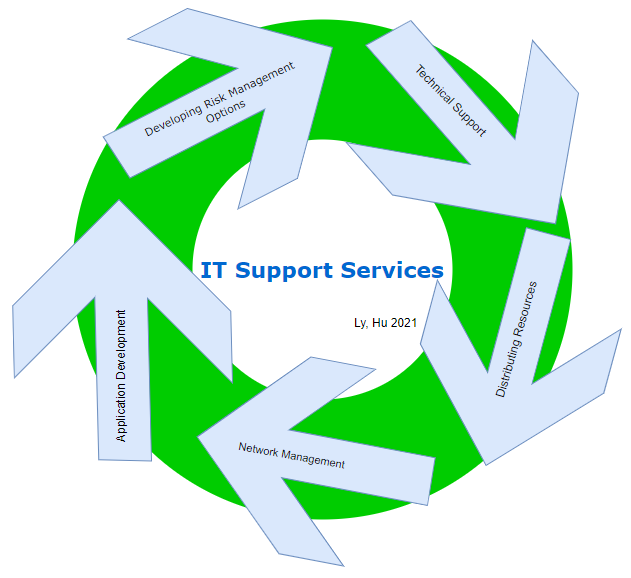
Due to the pandemic, DeepRock has chosen to make the decision to transition to a system that allows our employees to work from the comfort of their homes. However, this has provided attackers looking to access our network with a much larger range of targets who may potentially have networks that aren’t as secure. As mentioned earlier, one of the weakest links in our security chain is our employees. Much like for Goal #2, security awareness training must be set up that is specifically targeted towards remote employees to prepare them for attacks they may encounter. They must also be provided with guidelines for properly setting up their devices on their networks to ensure that their own networks are secure and able to defend against any attacks. Our next objective would be to then acquire a trusted VPN service to provide our employees with. This will allow our remote employees to securely connect to our network and gain access to the resources necessary to perform their jobs. Our final objective for this goal will be to ensure network segmentation is implemented. Should an attacker be able to gain unauthorized access to our network, DeepRock will be able to effectively reduce the damage that the attacker can cause through, as having our network properly segmented will ensure that the attacker will not have access to the entire network through a single point of entry.

**IT Philosophy**

DeepRock uses innovative information technology structures to fuel our consistent daily routine of handling holdings and business operations. The key objective of our systems is to provide our customers with the help they need in resolving any technical issues that they may face in either our games or our communication platform. Furthermore, these systems are utilized to provide support for our developers as well who face issues that may arise or require technical assistance in regards to setup or access.

To deliver these unique solutions, DeepRock’s facilities hinge on a mix of cloud foundations with the company’s business strategy. Moreover, sections of our infrastructure are presented to client’s units as Software-as-a-Service (SaaS). Some of DeepRock’s technology functions, such as their messaging network that is used to administer assets are outsourced and maintained by Computacenter. The company’s programs that oversee sales data are subcontracted to technology providers like SAP software.

Thus, DeepRock’s substantial faith in information technology services is vital in functioning the company’s everyday events. These everyday functions involve running fast distribution of resources, developing risk management options, managing the network, developing applications to serve core business needs, and delivering technical help with our platform for both our clients and members. These services and technologies are utilized to successfully accomplish DeepRock's mission.

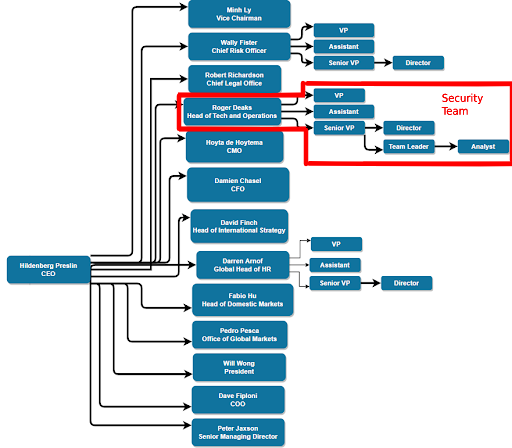


**Organization Chart and Reporting Structure**

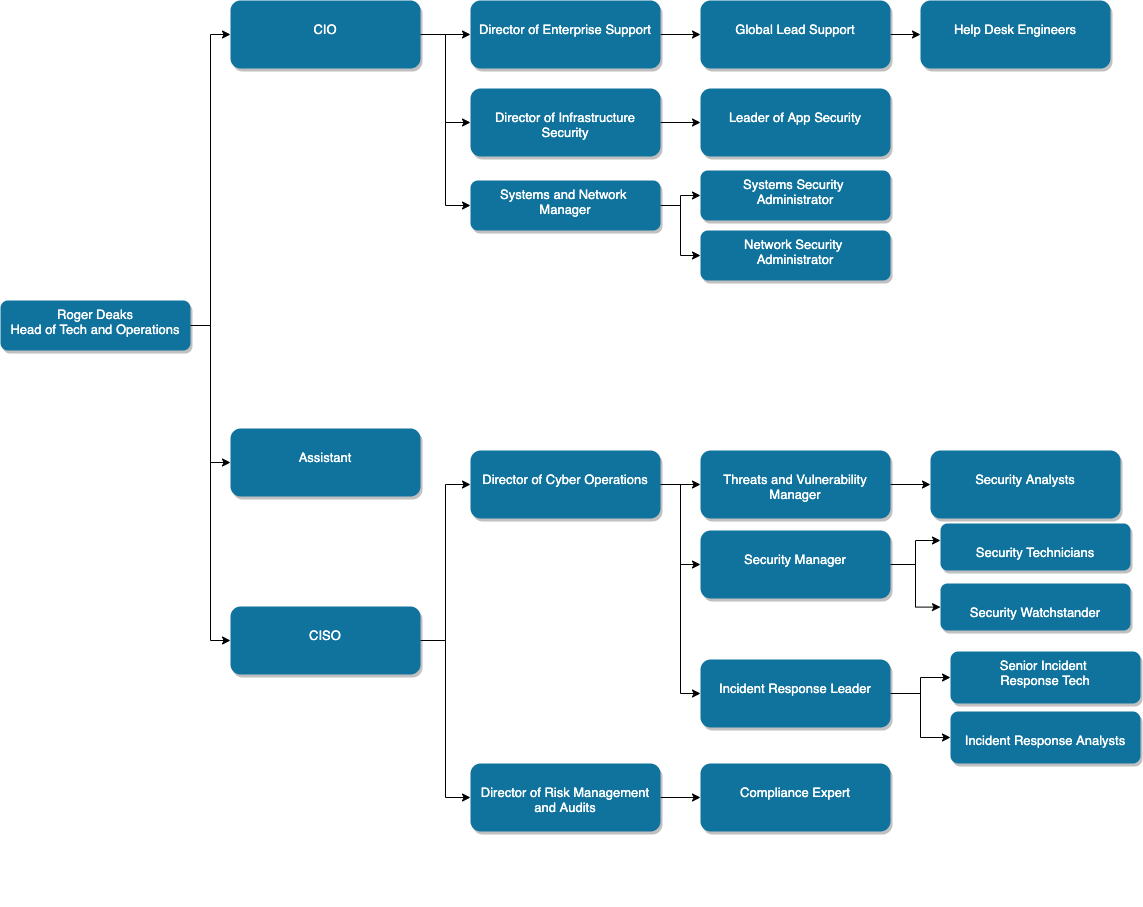
DeepRock is a growing organization of numerous members on the Board of Directors. Therefore, DeepRock’s organizational chart that is displayed centers on major positions in the firm. DeepRock’s organizational structure begins with our leadership unit who are tasked with our business functions, operations, and units, which are then shadowed by Vice Presidents, and Aides that report to them. Moreover, following the Vice Presidents, are Administrators overseeing divisions of the business. Administrators are then followed by engineers and company analysts responsible for daily observations and upkeep of company systems.

At DeepRock, our reporting structure enables groups within the company who are all vital to reach important goals of DeepRock. We have the appropriate assets to enable responsible directors to conduct their teams into delivering solutions. Our company can maintain a promotion of this reliability and create a secure future for all. Henceforth, the organizational structure administered within our company is ideal for us, allowing use to emphasize the company's calculated concerns and vision.

DeepRock Organizational Hierarchy



Security Team Hierarchy



**Security Organization Description**

The information security department plays a large role in the functionality at DeepRock due to the company’s dealings with both the personal and confidential information of its playerbase. Thus, it is a major component in developing successful services and products for DeepRock’s clients. The department holds true to DeepRock’s embedded philosophy in putting client’s protection first and maintaining network infrastructure safe from outside threats ranging from malicious equipment to groups.

DeepRock’s information security also takes care of defending company client and worker information found in computer systems, including various types of computer systems, USB drives, external drives, social media platforms and the numerous properties connected to DeepRock. Our information security unit requires these systems to be used in instances that benefit and relate to company operations and only to be used in regular DeepRock operating schedules. Moreover, to accomplish these set out goals, information security endorses DeepRock’s focused mission and vision on security and the statements in which the company has released. The department also sheds light on DeepRock’s core values which augment and enrich DeepRock’s program of cybersecurity for the future.

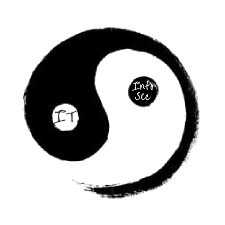
In order to avoid conflicting interests, the security roles are split amongst the IT division (consisting of CIO and below), (displayed in DeepRock’s organizational chart), and the InfoSec division (consisting of CISO and below). The heads of each division report to the Head of Tech and Operations, who in turn reports directly to the CEO.

DeepRock’s IT division has the task to supervise enterprise support. These tasks involve information security roles such as product security manufacturing, network security management, product engineering, and tech support assistance. Network security administrators play an especially important role as a part of DeepRock’s IT division, ensuring that DeepRock’s networks are not accessed by those without authorization. Furthermore, they provide technical support to employees, especially remote ones, in areas related to firewall or router setup for their home networks. If necessary, a few roles can function through the CIO subject to the regular company processes during the day.

The InfoSec division is accountable for tasks providing any coverage to the CISO. The unit oversees taking care of duties such as user access and identity organization, risk assessment of any third-party dealings, and confirming any compliance procedures found in global regulations. The group also holds up tasks with cyber actions such as managing incident response teams, tracking vulnerabilities, and overseeing the mitigation of threats. Positions under the Security Manager also play a crucial role in the InfoSec division. Security technicians provide the skills necessary to implement and administer new security technologies, while Security watchstanders provide the required monitoring and operation of these technologies. Moreover, the infosec department is continually working with DeepRock’s human resource sector to enlist proficient cybersecurity specialists that impart the same mindset as DeepRock’s.

The total sum of DeepRock’s security task force extends to around 300 and counting globally due its wide scale and intricacy of the information tech associated. As displayed in the chart, the construction of reporting within DeepRock’s infosec department supports the personnel’s requirements of a big organization like DeepRock. This support is done through successfully applying a separation of responsibilities and administering the division to make security determinations established on strategies and procedures incorporated with DeepRock’s organizational philosophy (Whitman & Mattord, 2018).

Likewise, DeepRock’s cybersecurity unit has an ample number of resources that is committed to supporting their team, which in turn maintains the growing trustworthiness and stronger security-based future for DeepRock’s users. Thus, the organizational structure displayed is an ideal arrangement for the group as it sustains the requirements to bolster DeepRock’s strategic image and concerns.

**Security Organization Justification**

Again, attributable to the substantial number of operations organized by DeepRock and IT systems employed to assist these activities, DeepRock has two groups of security functions. Our IT division is accountable for enterprise security and their information security purposes. As displayed in the cybersecurity team organizational chart, the unit consists of systems review, application defense manufacturing and desk support. These specialists certify protected and normalized software application procedures and systems functions. To go further, they also strive to grow in efficiency and guarantee compliance in DeepRock operations. Providing around the clock tech support for customers and personnel who are in need, elevates daily functions for ourselves and our consumers (Moore, Dynes, & Chang, 2015).

Our InfoSec division is accountable for management of security of our global IT holdings and technologies that the organization utilizes to perform business. As displayed in the cybersecurity team organizational chart above. This unit holds security roles in the Incident Response sector and Security Operations Center Analysts on numerous stages of support because of the varying IT assets being handled, necessitating numerous experts supervising each different level.

By choosing to separate these two divisions and have them report to the Head of Tech and Operations, we allow our IT division to focus on functionality and process and access information efficiently while our InfoSec division is free to examine our systems and technologies for any flaws without impeding the functions of the IT division. However, by having them report to the Head of Tech and Operations, they can still work together to accomplish the company’s goals. As an example, should the InfoSec division come up with new security policies, they can report to the Head of Tech and Operations who can then assign the IT division with the task of acquiring or developing the necessary tools to follow those policies.

Having our information technology sector being hybrid cloud-based with mixed computing and facilities made up of DeepRock’s infrastructure of data, and a public cloud consists of its own committed group. It has a physical security manager role since there is an established set of data centers and customer management platforms operated by customers, calling for thorough physical defense measures preserving compliance.

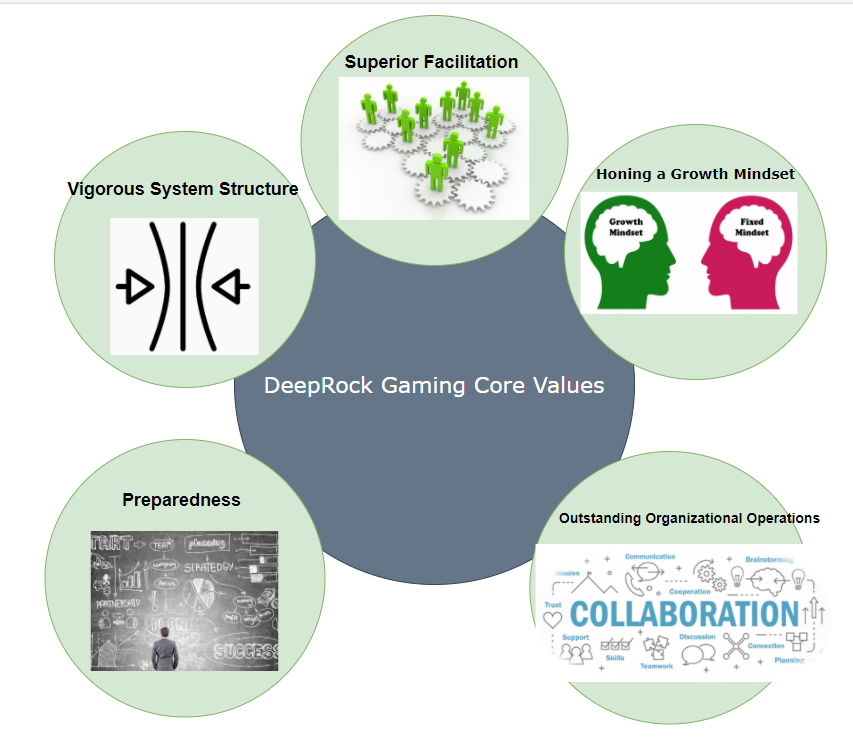
With the head of technology and the Chief Information Security Officer as lead, security positions such as risk assessment and other management roles manage assessment of DeepRock applications and products. Thus, it is the CISO’s job to verify that information security purposes are effectively operated at DeepRock. The CISO will not be in control of all security functions though. One instance is the role of the Chief Information Officer (CIO), who works with the enterprise staff, which is commanded by a director of enterprise support. A lower position that will take on security functions is the help desk specialist. These technicians will be able to support users who confront any security and technological issues. Therefore, duties can every so often be organized corresponding to a level that illustrates the target of a specific information security sector.

**Security Mission Statement**

The tasks and roles of the information security department are executed with the creed to recognize, evaluate, and take the initiative to direct DeepRock's information systems risks, which in turn will empower them to achieve its mission of establishing a safer outlook for their users.

**Security Core Values**

To succeed in our cybersecurity mission, we emplace these core values as the foundation of our company’s functions.



1. **Superior Facilitation:**

DeepRock views our users at the forefront of our services. Users are the first to be facilitated, which in turn, will certify that company operational quality is always growing in efficiency with the numerous company units backed by crews.

2. **Honing a Growth-Mindset:**

Learning from the past and utilizing a growth mindset is an integral core value embraced by all DeepRock. This value has additional facets that includes positive work environments driven by communicating intelligence amongst the numerous security roles. Quick responses are guaranteed with this value in place and cultivating this through the years will build a proactive attitude to the growing landscape of dangers that are encountered by DeepRock’s infrastructure (Dweck, 2009). Having a growth mindset is key to the advancements and innovations made at DeepRock. While the growth mindset concept wasn’t created primarily with business in mind, DeepRock CEO Hildenberg Preslin has embedded Dweck’s theories and concepts at every corner of the company. Carol Dweck is widely regarded as one of the world’s leading researchers in the fields of personality, social psychology, and developmental psychology. In Dweck’s early study, “A Social-Cognitive Approach to Motivation and Personality” (1988), she found that creating a “model specifies how individuals' implicit theories orient them toward particular goals and how these goals set up the different patterns” (Dweck & Leggett, 1988). In discovering these patterns regarding children’s behaviors, her research developed over time to concentrate on different groups of study such as adults in the business world. 

Dweck’s groundbreaking theory on the power of the mindset has a substantial influence on the abilities of students who possess growth mindsets to have higher motivation, higher comfort in risks, and higher performance levels. Dweck’s research involving the two different mindsets strongly influence workers who are not provided the proper teachings or environments from either the manager or any form of a boss. Dweck found multiple patterns that were strongly related to one another in relation to workers and their view of their own mindsets. Dweck states, “the mindset [mankind] holds about [their] abilities and intelligence can set them on different trajectories of motivation and learning” (Haimovitz & Dweck, 2017). Mindsets have a certain effect on employees' state of mind in regards to their potential, which has the possibility to be extremely powerful, especially for DeepRock, if pushed in the right direction. Dweck found that “[t]hese patterns are reflected in employees' achievement: Holding more of a growth mindset predict[s] [sic] better work performance, particularly for workers facing challenges” (Haimovitz & Dweck, 2017). The patterns of employees with a growth mindset leads to successful outcomes.

3. **Vigorous System Structure:**

DeepRock’s robust information technology setup is devised to be easily adaptable to fluctuations to any site, including in their own operational environment. In order to attain this level of success, scanning and assessment is a critical function within the cybersecurity unit of DeepRock. This unit aims to authenticate and guarantee that DeepRock technological system structures are capable of enduring various malicious pressures and incidents. There is a sense of focus when recognizing the vulnerabilities that are linked to systems that can potentially be attacked and manipulated at DeepRock. Scanning for any vulnerabilities is a must that is implemented by DeepRock so that we have the ability to classify the impact level to the vulnerabilities and guarantee accommodations are made to these vulnerabilities. The vulnerabilities involved are updated as new vulnerabilities are found. This permits our Cyber sector staff to address them as quickly as possible. Consistent testing is to be employed to find any existing vulnerabilities. This consistent and periodical testing provides in-depth analysis of weakness and allows for the staff to rank vulnerabilities. Proper testing could identify our gaming company’s resistance ability to any more attacks on data leak monitor services.

4.  **Outstanding Merit in Organizational Operations:**

DeepRock’s maintains a strong sense of focus on maintenance on their computer systems due to its dependability is of great value to their success. Therefore, the processes assumed in the information security division are to be undertaken while confirming the top readiness of the technologies are on hand. This would consist of a prioritization on the accessibility of services and utilizing the integrity of systems while meeting appropriate safety benchmarks. Team organization, communication, and commitment are necessary for DeepRock’s forward momentum and success. The whole company has a positive sense of urgency that is driven in passion for getting DeepRock projects on the ground and running. This is achieved through well formatted organizational operations which allows for personnel to perform their tasks efficiently and in a manner viewing their project in a bigger scope. Communication is key. Groups within DeepRock make sure to never have anyone feel in the dark and instead have everyone feel that they have someone to lean on when needed. Routines are set up that would result in the best feedback and products of personnel’s individual tasks.

5.  **Hope for the best, but are prepared for the worst:**

The aim of DeepRock’s information security division is to strongly store and safeguard the highest and lowest valued company assets and data, at any time through the months to years they are in DeepRock’s care. DeepRock seeks to earn users' trust with their relentless everyday pursuit to deliver secure comfort to an increasing quantity of users. While DeepRock values and trusts the system that they have incorporated, they are always prepared for the worst.

For a network wide defense to be successful, the work must start from within. Absolutely no system is automatically invulnerable from cyber threats. Neglecting this issue puts every asset's livelihood in danger. Our staff at DeepRock *must* have a proactive mindset in analyzing how to neutralize vulnerabilities and incoming threats, if not, we will always be one step behind. We must utilize guidelines from numerous cybersecurity frameworks that are available or construct our own to critically follow ideal practices and brainstorm to safeguard our assets on a daily and routine manner. Moreover, we cannot further stress the importance of our company’s and that we should be guided with the ability to discern symptoms and distinguish issues with in-depth defense. To be ahead of the enemy, we must engage in the proper forms of technology prior to any signs of activity that would put our data at risk.

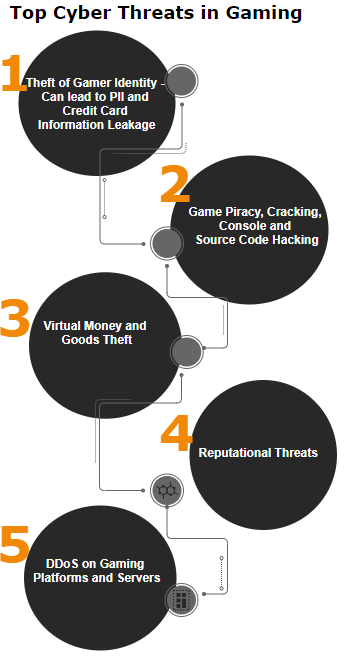
**Security Issues and Challenges:**



Due to DeepRock’s dealings with player data and payment information, they deal with numerous threats daily with changing and additions of assets from clients into DeepRock’s numerous databases. The laws and procedures fluctuating across the globe also hamper numerous issues that Deeprock must account for. The main risks for the company are found in dealings with DeepRock machineries, communications with third parties, and of course malicious cyber and physical breaches.

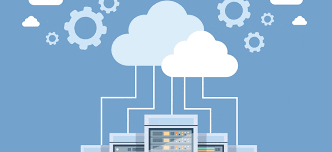
Consequently, DeepRock has continually stayed conscious of impending security threats and tasks on the horizon. The issues and challenges as stated in these next five points are present to the company today, and DeepRock has been responding to them and attempting to best mitigate them through data centers, policies, cameras, system security tools, detective, and recovery controls (Stewart, Tittel, & Chapple, 2008).

1. Cyber Breach Incidents: There are consistent threats on DeepRock’s workstation and transmission systems. These threats have the possibility of consequences and resulting in interferences on daily business operations and possible economic losses, including adjustment of intellectual or confidential data. These incidents usually occur from transmitted malware, social engineering, phishing, ransomware, or inadvertently caused by DeepRock’s very own employees. With a simple misclick or sharing of password information, employees can negatively affect DeepRock with damages caused from legal consequences. However, in DeepRock’s policies, there are security awareness training, included with an annual signature requirement signifying that they have reviewed and understood DeepRock’s policies has shown great improvement through the years at DeepRock (Brewer, 2016).

2. Complications with System Upgrades: An additional risk that DeepRock has is found within the process of upgrading their critical workstation systems. As stated before, DeepRock has a strong dependence on select major technologies such as the unique RK-N-STN OS and numerous other platforms to securely hold their data. The complete system upgrades, and safety procedures in position could possibly trigger interference and create numerous security concerns during the comprehensive system upgrade for DeepRock technologies. These issues could drag out around the globe at DeepRock locations may be followed by a stoppage of essential business operations including changing clients view on their trust for DeepRock (Hodge, 2011).

3. Issues with Third-party Interactions: Inaccessibility or malfunction of third party’s technological needs is an additional safety hurdle that DeepRock must overcome as a global business. This can dangerously impinge on DeepRock's indispensable merchandise: DeepRock OS. This lack of communication and negative response from third party work could essentially result in the loss of users, efficiency, thwart development, and influence DeepRock’s image as a brand. RK-N-STN OS hinges on contributions from a variety of third parties for assessment and projections of security threats and of course mitigation. The interruption of associated material movements may end in complexities in processes conducted by DeepRock’s OS. These worrisome interactions could also impede DeepRock's capacity to offer advisory security services to clients found internally and externally for the business.

4. Equipment Developments: There has been a continuous set of augmentations to RK-N-STN’s capabilities as an OS and its extension into different locational markets around the world. Through the last few years its processing range has increased substantially. This occurrence may in fact reveal DeepRock to larger amounts of scrutiny such as monitoring and heightened risk pertaining to information security, amount of operated data, and overall commercial operations. The business will be incapable to retain the program's operational stability and flexibility if DeepRock does not address this issue. This situation may cause a deficiency of new users, increased legal penalties or restrictions, and taint DeepRock and their OS’s image, altering profits and returns. (Manulis et al. 2020)

5. Virtualized Networks: DeepRock hosts a local hybrid cloud-based network within its organization and is utilized to deliver a secure private cloud case connectivity through company users, groups, and developers. This is key since DeepRock virtualized networks operate as a connection amongst information technology systems for managing daily operations. If these virtualized networks are cluttered with activity and are not correctly operating, company actions would be impeded, and core components would not be able to uphold their assigned positional responsibilities. The main exposure found in the usage of DeepRock virtualized networks is misconfiguration. Personnel could easily fall into making this mistake of inaccurate configuration of computer services with no defense hardening employed and leaving needless features left supported. It is imperative to not leave this issue unattended from first configuration since it is easily unnoticed in virtualized settings. Software that is applied in virtualization is typically set with default qualifications, and a variety of security hardening regulations deactivated for purposes like instant set-up, comfortable usage, and compatible control. These concerns could drag out across the globe at DeepRock locations may be followed by a stoppage of essential business operations including changing clients view on their trust for DeepRock.

**Conclusion:**

Some time ago, the necessity for information security was naturally deemed as a hollow expense to many companies around the world, however, that was before the commonality of data breaches worldwide. The modern pervasiveness of constant cyber-attacks on companies big and small has caused an insurmountable quantity of leaked information found in the public and in the black market. In the event of these breaches, companies are then pursued by serious charges for infringement of compliance standards and policies that they had failed to of course comply with. Therefore, the value of putting in place the cybersecurity plan that we have developed is only heightened and more prevalent than ever before. Information security is crucial for DeepRock’s mission as a company and must be implemented as a priority.

In this situation, we must capitalize on the opportunity for DeepRock’s global business actions. Having the framework for this cybersecurity plan, effectively utilizes information security and necessary digital mechanisms to grow in production, user insight, worker engagement, and an advantage over our competitors. All these factors have been assimilated into the company's recommended strategic cybersecurity management plan.

The recommendations stated throughout the plan could offer our corporation with improved network security permitting the company to defend their organizations confidentiality and integrity of their network. In the strategic security plan, the mentioned methods are for us to develop its strategic security to back the numerous business purposes. Our plan’s techniques, if used properly, can give the company the capability to integrate a risk-based approach and distinguish security incidents and respond to an incident in a swift and effective manner. With an optimized network security supplemented with software patches that are up to date and hardware security, this will avert the organization from falling to any of these malicious types of attacks (Mayer, Wool & Ziskind, 2000).

A properly established and formatted security control system, the organization should also be aware that they need to implement a security cognizant workforce that will have the ability to generate and preserve strong passwords, dodge any malicious applications, and certify sensitive data is not stolen.

The first part of our strategic cybersecurity management plan for DeepRock has a goal to retain our organization's security sustainability and to be readily equipped for the possibility of any malicious occurrences that could happen in the field of information security. The plan is also developed to make certain that crucial business operations will remain functioning even in the event of unforeseen emergencies. Accordingly, to accomplish these objectives, recurrent support is imperative from directors to focus on the essential fields that have been discussed. These fields include forming security-conscious personnel and growing with retained members for the significantly expanding size of our company.

**References:**

Ltd, K. (2021, January 20). Humans are the weakest link in the information security chain. Retrieved February 09, 2021, from [Here](https://kratikal.medium.com/humans-are-the-weakest-links-in-cyber-security-of-any-organisation-ac04c6e6e71#:~:text=You%20already%20know%20the%20weakest,security%20repercussions%20for%20their%20organizations)

Brewer, R. (2016). Ransomware attacks: Detection, prevention and cure. *Network Security, 2016*(9), 5-9. Retrieved from: [Here](https://www.sciencedirect.com/science/article/abs/pii/S1353485816300861)

Dweck, C. S. (2009). Mindsets: Developing talent through a growth mindset. *Olympic Coach, 21*(1), 4-7. Retrieved from: [Here](http://assets.ngin.com.s3.amazonaws.com/attachments/document/0005/2397/Mindsets.pdf)

Haimovitz, K., & Dweck, C. S. (2017). The origins of children's growth and fixed mindsets: New research and a new proposal*, 88*(6), 1849-1859. Retrieved from: [Here](http://web.a.ebscohost.com/ehost/detail/detail?vid=3&sid=c32d5c10-9ff6-4afb-9f07ab42a40667e3%40sessionmgr4006&bdata=JmF1dGh0eXBlPXNzbyZjdXN0aWQ9czkwMDg2NTUmc2l0ZT1laG9zdC1saXZlJnNjb3BlPXNpdGU%3d#AN=EJ1159962&db=eric)

Hodge, P. (2011). Virtualization 101: Understanding how to do more with less. *System,* Retrieved from: [Here](https://isajobs.isa.org/standards-and-publications/isa-publications/intech-magazine/2011/august/system-integration-virtualization-101-understanding-how-to-do-more-with-less/)

Manulis, M., Bridges, C., Harrison, R., Sekar, V., & Davis, A. (2020). Cyber security in new space: Analysis of threats, key enabling technologies and challenges. *International Journal of Information Security,* , 1-25. Retrieved from: [Here](https://link.springer.com/content/pdf/10.1007/s10207-020-00503-w.pdf)

Mayer, A., Wool, A., & Ziskind, E. (2000). Fang: A firewall analysis engine. Paper presented at the *Proceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000,* 177-187.

Moore, T., Dynes, S., & Chang, F. R. (2015). Identifying how firms manage cybersecurity investment. *Available: Southern Methodist University.* Retrieved from*:* [*Http://blog.Smu.edu/research/files/2015/10/SMU-IBM.Pdf*](http://blog.smu.edu/research/files/2015/10/SMU-IBM.Pdf)

Stewart, J. M., Tittel, E., & Chapple, M. (2008). *CISSP: Certified information systems security professional study guide* John Wiley & Sons. Retrieved from: [Here](https://books.google.com/books?hl=en&lr=&id=YwZYZbsl2GEC&oi=fnd&pg=PR7&dq=data+centers,+policies,+cameras,+system+security+tools,+detective,+and+recovery+controls+%27&ots=WQA1hPQEvI&sig=GAJZiNkdCY_aLWhyD8hJn1VA7KQ#v=onepage&q&f=false)

Whitman, M. E., & Mattord, H. J. (2018). Management of Information Security, 6th Edition Retrieved from: Online Copy