**DeepRock Security Inc. Strategic Cybersecurity Final Plan**

**Minh Ly**

**Favier Hu**

**University of Dallas**

CYBS 8396 – Strategic Cybersecurity Practicum

Spring 2021

Dr. Sandra Blanke



Abstract......................................................................................................... 3

Security Metrics.............................................................................................. 4

Business Continuity Strategy............................................................................ 8

Disaster Recovery Plan.................................................................................... 11

Security Staffing Strategy................................................................................ 11

Security Position Job Posting............................................................................ 14

Security Awareness Plan.................................................................................. 16

Security Newsletter......................................................................................... 18

Budget.......................................................................................................... 19

Executive Summary........................................................................................ 21

References.................................................................................................... 22

**Abstract:**

There is an understanding of our users and stakeholders fears in defending their private data that is collected and distributed within our company bounds to operate our daily tasks. Therefore, we have pressed data security to the vanguard of our company's ground plan to account for the new cyber landscape filled with countless malicious individuals and entities.

This detailed plan is conscripted to achieve a two-part strategic cybersecurity management proposal for DeepRock Gaming Inc. with the goal of maintaining the company’s defense measures and vigilance for possible breaches or threats that could occur in their data security sector. Our proposal starts with security metrics utilized to assess the efficacy of the current data security plan through pursuing cost associated practices to amplify execution in association with DeepRock’s company principles.Next, the strategies for business continuity and disaster recovery are focused on since it has a strong relation to security threat events. A model directive is defined for disaster situations. Successively, the essential procedure of employing a data security unit for DeepRock is tackled, alongside a model position posting for a position in the security unit. Lastly, the subject of security instruction is reviewed with recommended issues to be included in training. A model newsletter is offered to maintain workers’ security awareness.

United with DeepRock's leadership unit, our comprehensive strategic cybersecurity plan is endorsed for approval. Its intention is to steer the security operations at DeepRock to greater lengths and provide a powerful foundation to develop and generate wide-ranging cybersecurity processes for DeepRoc Gaming Inc.

Sincerely,

*Minh Ly and Favier Hu*

CISO and Management Director

**Security Metrics**

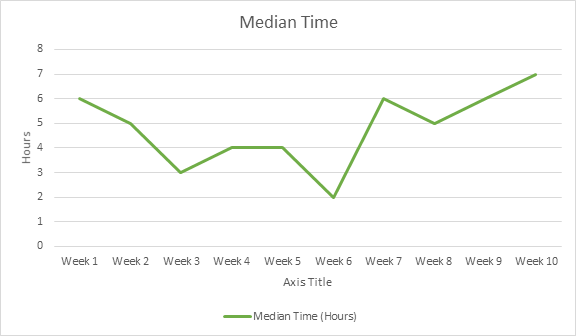
In order to certify that our plan is successful, security measurements will have to be identified to provide us a track to follow. This would be done through using security data tables, which offer useful intelligence on the functionality and overall success of DeepRock’s cybersecurity unit. “[Metrics] allow[sic] security team[s] to better communicate on the organization’s security posture, describe threats and vulnerabilities, present a ‘plan of action,’ and get a pulse on the organization’s risk tolerance (Baskerville, S. 2017)”. It would also support leaders by helping them make proper risk interchanging decisions. What will soon be displayed are metrics linked with our proposal that evaluates the efficacy of the recommended cybersecurity management proposal for DeepRock.

1. **Credential Modification Time:**

A measurement that will be followed and described is the duration for any of our users to change personal PIN, password, or passphrases to gain admittance to their individual DeepRock Gaming profiles. In addition to this access is the collective IT services such as the Active Directory.

This particular metric has been stored because of the loss in production when sections around the globe for our users are sealed from their DeepRock account. Once locked, these users are unable to complete any actions within the DeepRock platform, restricting any payments or activity with other users. This will impact the fiscal value of our company and to a level, economic losses, because of the possible in game payments made as they await to gain reestablished access.

The data utilized to trace this specific metric will help enhance the key source admittance process speed through changing users’ passwords. This will also help offer understanding on the importance of implementing a security purpose like this, which reduces loading and reset time, reducing monetary damage. The audience for this metric would be our Systems and Network Manager, Security access Manager and our Director of Infrastructure Security since they would be able to advise valuable approaches for where developments could be done. We propose that this metric be gathered weekly and be submitted every 3 months for evaluation. Security analyst specialists will be partnering with system and network admins for collection, analysis, and reporting of the metrics. This security metric is pictured below.

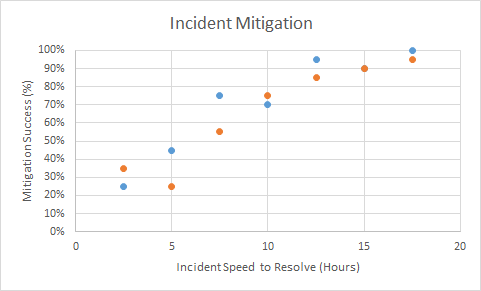


2) **Incident Mitigation Speed:**

The next metric that is followed and described is the speed and time in which mitigation is applied to any security incidents linked to business devices. Workstation desktops and laptops are valued resources at DeepRock which are utilized by employees frequently to work with internal servers, including numerous other networks consisting of classified information. “Any higher level designer would give an opinion that online servers are the easiest target. It is also the most targeted due to the amount of sensitive data it holds (Infotech, N. 2021).

The metric being constructed operates as a marker of the importance of DeepRock’s infosec plan and is utilized to follow and develop the mitigation procedure of incidents for DeepRock’s devices. Moreover, it will be used to communicate the security knowledge of employees alongside possible production and monetary loss sustained as a consequence of the mechanisms that are in focus.

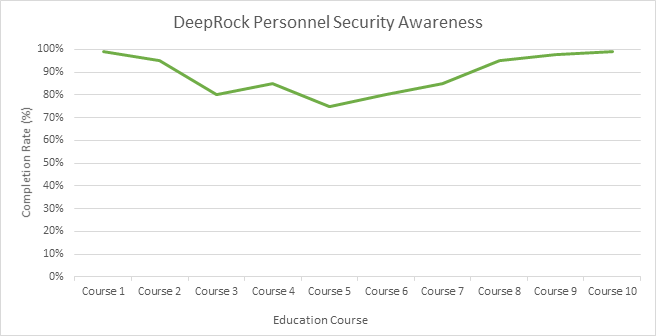
The audience for this particular metric will be our incidence response leader and the Director of enterprise support since they would jointly mix together to mitigate DeepRock security incidents regarding workstation devices. This will be accumulated every day for each hour of the day and submitted each month. Senior Incident Response techs, security analysts and technicians will be accountable for collection, analysis, and reportage of this metric. This security metric is pictured below.



3) **Company Awareness Level:**

Our third metric consists of the achievement ratio of security awareness training. This metric is a guide for the security awareness position found at DeepRock from the viewpoint of social engineering. It is also a valuable device for audit functionalities as it will assist DeepRock’s leadership unit in evaluating DeepRock’s compliance concerning consistently planned workforce education.

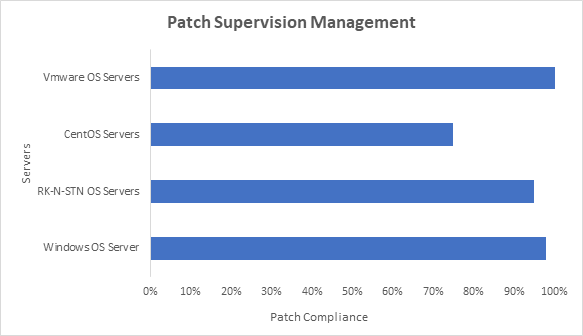
Furthermore, this metric is utilized to quantify the efficacy of DeepRock’s campaign for the growth in security cognizance and assists in recognizing development in specific parts. An example of this lies in managing tough evaluations or employing various methods to gather the workers' performances in their individualized comprehension of security efforts.

The audience for this specific metric would be DeepRock’s active Chief Information Security Officer (CISO). Each time an awareness training is distributed, collection of the data metrics will be made. Every three months, the collections from the number of campaigns done within these three months will be displayed. Our Program Director of Education who operates directly with DeepRock’s training sector will be responsible for collection, analysis, and reportage. This security metric is pictured below.

4) **Managing Patch Supervision:**

Our next metric is focused on patch program compliance for DeepRock company servers. The information for this metric is gathered weekly and registered every month to the company database. The information collected for the metric displays DeepRock’s risk posture and aids in tracing vulnerabilities which occur on key company systems. Furthermore, it operates as a marker of DeepRock compliance for servers when related to DeepRock’s patch procedures. This metric is computed through linking the amount of entirely compliant systems alongside servers going through the patch managing. Metric system is displayed through zero to one hundred.

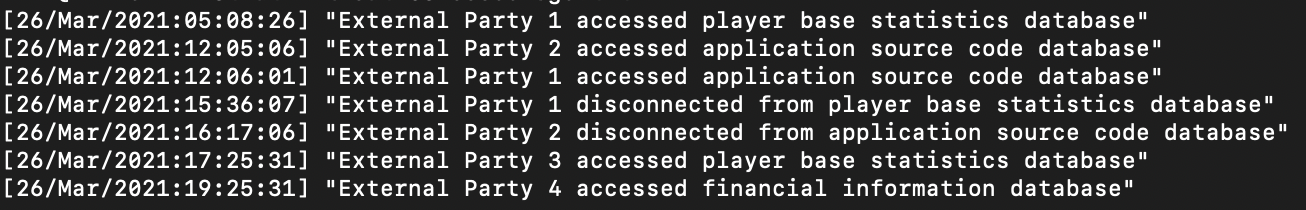
The computations from this metric will also help DeepRock’s patch managing agenda's efficacy. The information recognizes fields for development, as well as regions where assets are greatly needed to increase. This method will assist in any forms of compliance inspections through demonstrating that DeepRock is following relevant guidelines and regulations. Additionally, this metric could demonstrate the company's risk tolerance assessments concerning patch supervision. The audience for this would be company System Analysts, System and Network Manager, Infrastructure Security Director, System Security Admin, and compliance experts. Vulnerability and Security management will be responsible for collection, analysis, and reportage who will supervise resource tracing and imaging devices. This security metric is pictured below.



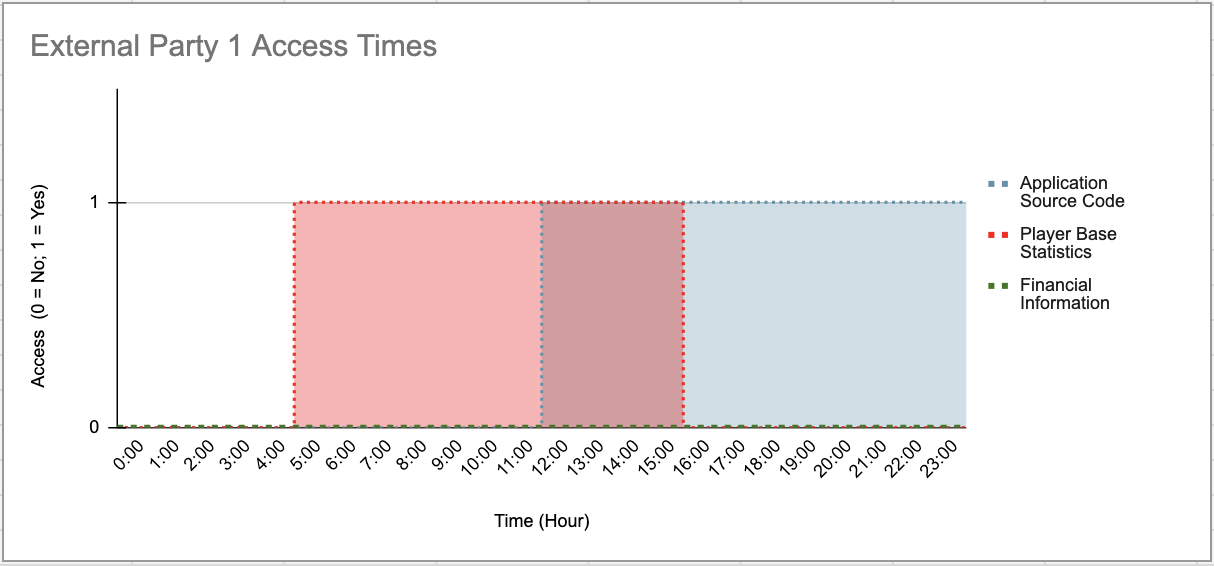
5)  **Critical Systems Access Times**

The last metric that will be tracked are the times that any systems containing critical information are accessed and by whom. Due to the size of our company, there may be situations where we may need to strategically partner with multiple third-parties in order to achieve certain goals. This would result in situations where they may require access to those critical systems contained on our servers in order to work with us. By keeping a log of which external parties are accessing our systems as well as the time and system that they are accessing, we will be able to pinpoint a possible area of vulnerability within our systems due to a third-party’s access in the event of a breach.

This metric will be continuously collected and analyzed using software rather than through manual methods. Reports generated from the software analysis of the collected information will then be reported at the end of the day to both security watchstanders and security technicians. An example of the data collected can be seen in the sample log file below.



From this log file, an access report will be generated for each external party that can be further analyzed by both security watchstanders and security technicians. Below is a sample access report that will be viewed by security staff.



**Business Continuity Strategy**

DeepRock depends on our innovative data technology systems to reach our daily processes along with fueling asset management company products. The main objective of these systems contained by DeepRock Gaming is to produce an excellent form of gaming and socialization platform for consumers by linking them to our services, guiding the digitalization of their information and connectivity across the globe regardless of their location. Nevertheless, in the realm of InfoSec, nothing is entirely certain to be accessible to us at any time. Therefore, a business continuity strategy plan is included in this plan for DeepRock to “cop[e] in a crisis easier. It will also enable [us] to minimise disruption to [our] business and customers, often at the expense of competitors. It is a way of proving to customers, insurers and investors that [our] business is robust enough to cope with anything that might occur (Nibusinessinfo., 2021)”.

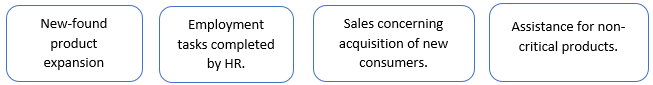
DeepRock’s Business Continuity Plan will be supervised and operated by our CEO and COO. In congruence with DeepRock disaster recovery processes, the (BCP) will be implemented. Our strategy’s main purpose is to make certain that vital company processes will remain functional even in the occurrence of any crises.

In order for DeepRock to be successful in minimizing loss to our revenue, a strategy utilizing a backup company hot site will be followed. This would be an alternate location where DeepRock’s processes could continue for the duration of a given disaster. The spot would contain all essential gear and workstations, with backup data, PCs, mobile phones, and any associated tools for DeepRock to persist. This planned hot site is vital for DeepRock’s delicate landscape regarding the constant usage of the platform with users and our services. Even five minutes of interruption for our platform will not go unnoticed and could be completely catastrophic since all users of DeepRock’s services will fail to view any assets and capability to execute any functions with other users and their own properties. This failure would result in severe financial losses for DeepRock. Thus, elevated accessibility will be formatted within the location, with completely functioning balanced systems and hourly information being reported from the host site.

DeepRock’s continuity strategy will be employed to all of our high-ranking assets stated in our risk management plan such as RK-N-STN OS, staff, products, archives, Cloud-Based servers, phones, workplaces, networks, and other crucial services found at DeepRock. The assets stated are included in delivering gaming platform managing services for users which create the bulk of DeepRock’s gains and sustain processes are performed. Key operations in capacity for continuity are reviewed below.

| **Company Action** | **Summary** |
| --- | --- |
| Assistance to Users | * Key roadmap to maintain delivering services and reach service-level agreement conditions. |
| Assistance for DeepRock Equipment Services | * Managing incident response units and actions. * Company risk and directorial review. * Examining existing processing assets. * Continuous induction of devices and products. * Implementing enhancements and updates on present structures. * System HR company payroll. |
| Networking | * Company media assistance for users and workforce to retain functions and maintain updates. * Support to work out problems by contacting field specialists/operators. |
| Implemented Failover Methods | * Charting computer and software systems to be employed to attain the needs for essential company processes. * Complete reproduction and imagery of hot site workstation assets to permit instant system failover initiation and low interruption during a given emergency. |

Conversely, the following purposes have been listed as non-crucial functions. Therefore, they are outside the range for DeepRock continuity strategy.



Moreover, the major administrative members at DeepRock in executing our business continuity scheme are stated and reviewed below.

| **Positions** | **Tasks** |
| --- | --- |
| Chief Executive Officer | * Has a major responsibility in critical judgments and procedures of DeepRock’s business continuity strategy. This includes meeting with heads of numerous management divisions and the board about disruptive incidents and recuperation length. He/she is additionally accountable for certifying that DeepRock’s recovery unit gets the required assets and backing to achieve their designated jobs. |
| Chief Operating Officer | * Validates crucial company procedures, facilities, operative tasks, and machinery are accessible to restart business processes. |
| Head of Tech and Operations | * Manages the complete accountability of DeepRock’s data structures and the critical functions within. |
| Administrators | * Responsible for the management of company processes that are dependent on data work systems. |
| InfoSec Engineers | * Accountable for defensive actions engaged in improving, applying, and preserving data structures. |
| Recovery Units | * In charge of fulfilling their designated tasks and responsibilities in the essential company sectors. |

Ultimately, our business continuity plan will be assessed on four occasions throughout the year through the use of an assignment where delegated responsibilities and proper proposals will be allocated to recognized persons within DeepRock. With this procedure, a demonstration of the strategy is performed to assess if the processes will indeed function as they are planned to, whilst probing and drawing attention to any disparities. Furthermore, a mock-up drill will be delivered each year. This would comprise an exercise in which individuals will play roles as if a genuine emergency had arisen at DeepRock. The company’s hot site will also be assessed for required operational facilities, involving departure and transmissions. After these tests are finished and findings are drawn, a report will be developed on the drills, alongside a suggested forthcoming training program to head executives and directors. It will additionally be utilized for any revisions to better the strategy.

**Disaster Recovery Plan**

Strongly associated with our business continuity plan, our disaster recovery plan works as a key position in returning the complete company to maximum capabilities following a disaster. Planning for such catastrophes can be measured in company action, such as, by analyzing the recovery of DeepRock’s servers running the RK-N-STN OS, a high-ranking property as recognized in our risk management file. “Disaster recovery planning [at] [DeepRock] enables [us] to maintain a high service quality, regardless of the circumstances. Reacquiring an old customer in the aftermath of an IT disaster can be nearly impossible [in] [gaming] (IP, E. 2018)”. This asset is utilized to operate user profiles and directories by managing the user interfaces components consisting of numerous inner applications (games, news update, climate, friends, and tech). Thus, it offers a substantial revenue supply and includes confidential data utilized in even the smallest user and admin operations, such as user card records for registration.

A few of the main measures that must be carried out prior to regaining DeepRock’s servers are:

1. Create a platform in which the focus is having the service accessible to users rather than on features such as software enhancement or assessment.

2. Ensure DeepRock’s business continuity strategy is readily functioning, with the developed hot site prepared.

3. Backup DeepRock’s servers which contain critical information such as DeepRock’s application source code and player’s login credentials and payment information on a daily basis to DeepRock’s hot site, enabling the hot site to be readily available and utilized at any minute.

4. Conduct live emulation of DeepRock facilities and established applications. Also, ensure databases utilized in DeepRock’s core system are reflected in a trusted cloud memory space.

Subsequent to our stated proposals, the DeepRock Server Unit, which is composed of our Application Database Supervisor, Server Admins, and Network Admins, will execute the recuperation process. Their corresponding directors will be in charge of the reestablishment with the leadership of the Chief of Enterprise Support and CIO. Multiple emergency equipment and supplies (flashlights, fire extinguishers, first aid kits, etc.) will be provided as well to aid in the recovery process along with a detailed map of the layout of our primary facility and the locations of all emergency equipment and supplies.

# **Security Staffing Strategy**

Having the ability to appeal, employ, and keep a highly creative workforce is crucial for DeepRock's presence and accomplishment. Therefore, we have constructed a security recruitment plan which is integrated for DeepRock to apply in tackling the important and delicate procedure of enlisting, employing, overseeing, and dismissing personnel. The constructed chart below reviews numerous methods for DeepRock to employ.

| **Method of Employment** | **Explanation** |
| --- | --- |
| Worker Recommendations | Current DeepRock personnel would be capable of recognizing appropriate applicants for numerous positions because of their thorough understanding of the philosophy and operational environment. These personnel would initially have to confirm understanding of DeepRock's numerous policies regarding corruption during the procedure of recommendations, which negates any possible thought of hiring in a nepotistic method. |
| Public Position Submission Gateway | Interested individuals could submit an application for the positions they believe they are suitable for electronically on DeepRock’s hub. When submitted, the employment unit will assess the application prior to progressing further in employment. |
| Virtual Position Sheets | DeepRock takes candidates via numerous websites such as LinkedIn, Glassdoor, and the quickly growing Indeed. DeepRock’s online position sheets will offer admission to a substantial group of applicants that our employment unit will assess prior to progressing further in employment. |
| Recruitment Organizations | Recruitment organizations carry out vetting activities and aim to fit applicants with a company's available positions. Nonetheless, these organizations are deemed the lowest method in exploring for applicants because of the high expenses related to the recruitment of applicants. |

Our defense unit largely considers technical abilities during the process, such as the ability to troubleshoot basic network problems on hardware or software and design information security plans (Zippia, 2021). These proficiencies are highly essential as these are the abilities necessary to successfully carry out the given tasks. They also lower the teaching obligations necessary for a selected applicant updated on DeepRock’s tasks. Therefore, a benchmark of instruction and accreditations are mandatory according to the Department of Defense recommendations. This prerequisite consists of Systems Security Licensed Specialist, amongst numerous other certifications, with also the necessity of Networking expertise. These competences can additionally be accompanied with a degree from a certified establishment, with a standard bachelor’s or Master’s degree in IT, concentrating in cybersecurity.

Soft skills like efficient communication are quite critical since functioning in the defense unit entails work in partnership with numerous people within and outside the field of IT and will have to accommodate for personnel’s low technical knowledge in comparison to the specialists found at DeepRock. “These tasks allow the organization to identify the work role(s) and specialty area(s) that are gaps” (Newhouse et al. pg.17, 2017). Furthermore, DeepRock as a company necessitates coordinating with customers and industry experts, so the need for first-rate communication proficiencies is indispensable to clarify methodological specifics to administrators, executives, and the board and in addition working well with associates and customers.

From our research we found that “while there is no hard and fast rule, aiming for between one and three interviews, depending on the level of the position, is a wise move” (TrcStaffing., 2021)”. Procedures that are utilized in the interview process are described in the constructed table.

| **Interview Method** | **Explanation** |
| --- | --- |
| Preliminary Video/Voice Conference Meeting | Applicants will principally get tested through a voice/voice call to assess their curiosity in the position they requested and to confirm the individual has the requisites for the position through the use of their resume. |
| Second Video Conference Meeting | After accomplishing the preliminary inspection, the applicant will then be assessed for their technological abilities, competence, and capability to converse and express understanding with DeepRock interviewers. The meeting will assist in deciding if the applicant's professional pursuits affiliate with DeepRock’s and the unit's long-standing wishes. |
| Third and Final Conference Meeting | Once verifying that the applicant possesses the necessary skills and has aligned job pursuits with DeepRock’s desires, this final meeting is performed by security administrators to decide if the nominee is capable to conduct the position-limited responsibilities needed. |

If the applicant is considered as an ideal match for DeepRock’s position on the defense unit, a formal agreement document is then sent to the applicant with a minimum time to reply. If the individual agrees to the document, the means to join the team commences with a directory of following measures transmitted by DeepRock’s Human Resources sector. A non-disclosure agreement must also be signed to comply with DeepRock guidelines.

DeepRock’s strong offering of benefits will draw sharp applicants, these include:

* Offering competitive wages within comparable industry positions.
* Matching up to 6% 401(k) plan.
* Training repayment plans and Kaiser medical coverage.
* Paid time off, sick and holiday periods.

When the applicants are officially accepted, they will then be educated with a variety of methods, such as shadowing. A few other examples are through DeepRock developed teaching virtual gateway, where administrators can designate the applicant’s resources to fulfill. More examples of teaching methods are through company training websites like Udemy and Linux Academy, which provide rich material for our new hires. Proper free training resources can also be distributed by Sans the U.S Department of Homeland Security.

In order to keep our newly hired security personnel and cut down our turnover ratio, we have constructed a strategy to retain them.

* Exclusive offers for instance advanced security programs, free admission to numerous security symposiums located over the nation which will be reimbursed.
* In light of COVID, we will offer at least two days during the week to work from home after one is able to complete all standard training courses found in the first four months being on site.
* Promotions for personnel when called for in their projects or achievements will provide support in their work evaluation and development.
* Bonuses will be provided after 2 years of work that consist of 5% of their base salary (No major faults are done by the employee). Will display to personnel that the individual and group projects in which they are doing are respected.

Lastly, on the occasion in which an employee from the security sector leaves DeepRock, the strategy utilized for employing security staffing incorporates the delicate procedure when dismissing employees from their position. Therefore, we have developed processes which could be used as a plan for these events.

* The personnel’s administrator, unit, and human resources must be informed on the specific personnel’s departure. Varying on the situation (responsive or tough) departure, the ex-personnel’s admission to any of DeepRock’s assets will be ceased when the notice of their departure is enacted.
* They are needed to send back any DeepRock assets, ie. Access card, computer, keys, and any non-confidential or confidential physical/digital files or information. Their DeepRock company hard drive will be obtained.
* All of the employee’s door and storage access locks will be altered in case of any return.
* All private possessions will be confiscated from DeepRock grounds after the first two days.

**Security Position Job Posting**

A model position report in association with DeepRock’s employment strategy has been constructed below. In the description below, it lists the abilities that are essential to carry out the responsibilities of the position. The model that is displayed refers to a Stage I Security Technician job opportunity.

Job Summary:

Position Name: Security Technician Tier I

Position Manager: Security Unit Manager

Location: Hayward, California, US

Position Identification Code: 6030

Date of Publishing: 3/19/21

Job Information:

The Security Technician Tier I position involves delivering assistance to threat occurrences and observing records for assigned data systems. Moreover, the person assigned this position is accountable for identifying/troubleshooting network problems, collaborating with the IT team to set up arrangements so that systems can be recovered quickly, designing information security plans, and extending support to help in carrying out the security strategies.

Necessary Qualifications:

* Bachelor’s or master’s degree with at least a concentration in cybersecurity.
* At least one year with involvement in a position related to the sector of incident response (preferably with source code defense).
* Familiarity with defensive devices for instance firewalls or SIEMs to name a few.
* Familiarity with fundamental networking practices and essential services.
* Understanding of SQL and/or Python
* Meticulous, capable of functioning at a high rate of multitasking and organized rapidly moving work atmosphere.
* Strong interactive abilities and listening to work members. Verbal and writing merit.

Tasks:

* Once notified of any possible security threats on specific hardware, you will either speak over the phone or work on site to distinguish and mitigate the threat found in the network security of the given material.
* Define the core origin of a security threat on hardware/software and construct approaches to mediate.
* File any cyber security cases from preliminary recognition all the way through to the definitive solution.
* Complete numerous malwares testing on possibly breached documents or devices to collect markers of issues.
* Maintain and repair security-related concerns at DeepRock.
* Identify and troubleshoot network related issues on hardware or software.
* When identifying numerous files, technicians will discern feasible mitigation and remediation strategies.

Where Do I Apply for a Position?

Apply for the position at DeepRock career listings website gateway listed below! [https://careerlistings.DeepRockGamingInc.com](https://careerlistings.deeprockgaminginc.com)

About DeepRock:

As an international company, DeepRock Gaming Inc. combines customers' social needs with their gaming needs. Our databases and network configurations are located in six continents and have employed 8,800 experienced specialists at our departments found in over 15 nations. We are quickly becoming one of the biggest gaming and social media platforms in the world. Our approach to gaming and developing games is unique in providing solutions for our users’ needs through use of a completely optimal user-friendly interface.

All through our 15 years as a growing company, we have continually placed our users at the forefront of our services. Our user’s wishes are imperative to our continuous growth as a company, so we perform at a high level to provide. The customers are our gateway to learn what needs to be improved. We gain major insights from our users located all around the globe and we use this global grasp to provide outstanding accomplishment in all our gaming industry conditions. We at DeepRock intend to be the finest in accomplishing an equilibrium across all continents when it comes to social media and gaming.

**Security Awareness Plan**

An essential method to create and preserve security procedures inside a company is to train personnel and sustain their understanding of data security mechanisms. Therefore, we have developed a portion of our strategic plan to account for security employment perception strategy for DeepRock to apply and assist personnel to fully comprehend their positions and tasks associated with DeepRock’s cybersecurity. “Cyber security starts with [our] employees. [We] must motivate [our] employees to want to learn about cyber security threats and risks (TerranovaSecurity, 2021)”.

Our employee security education plan will consist of three core parts listed and described below.

1) Common Worker Instruction: This first part will involve matters that will relate to all personnel and independents. It will contain subjects for example information protection, management of pins, ideal forms of performing tasks, and practices when creating a report for infringement of DeepRock security.

2) Organizational Instruction:This instruction focuses on administrators and involves material such as overseeing specific admission management, security concerns when enabling entry to assets, and management choices.

3) Specialized Instruction:This instruction is designed for information technology professionals and system security supervisors/analysts. It encompasses complex technological substances appropriate to their intricate tasks. It also features material concerning the devices they will operate or oversee.

Numerous crucial topics will be encompassed through the developed data security education curriculum, these are listed and described below:

1) Cyber Conduct and Behavior:For this subject, personnel will be informed on how to make use of the internet to properly gain access to company assets. This involves averting any possible deceitful (spoofed) systems. It will also recognize the significance of linking to DeepRock formatted cloud-based networks and vpn’s. Lastly, this topic will finish with going over best practices for using robust password methods and why one needs to consistently patch their software and appliances.

2) Threat of Social Engineering: Personnel will be trained on how to distinguish and alleviate any possible social engineering methods being done towards them or another. This involves detecting any malicious emails/messages of phishing and also any physical defense issues. “[H]uman error or weakness to gain access to any system despite the layers of defensive security controls that have been implemented via software or hardware” will be worked on with this subject (Gulati pg. 3, 2003). This seeks to prevent any assailants from being successful by educating a staff that is conscious of their surroundings physically and in the digital world. They will be able to deduce situations and permit them to notify the appropriate groups to account for the matter.

3) Information and Malicious Software:Personnel will be trained to identify and understand the harm that malware can do to DeepRock’s confidential information and database software. Workers will “be on the lookout for both identity theft and credit card fraud, check in with your account balances and credit score regularly. Several services offer free ID theft monitoring, credit monitoring, and questionable credit charges. [One] can even use Google Alerts as an identity theft watchdog (Kumar, Chaudhary & Kumar pg. 17, 2015)”. This involves recognizing the actions done by specific computer viruses, circumventing malware, consistently planned file duplications, scanning for any viruses, recognizing safe sites, and averting transfers from sites other than DeepRock’s facility.

We have formulated methods which will communicate our stated security instruction, which are described below:

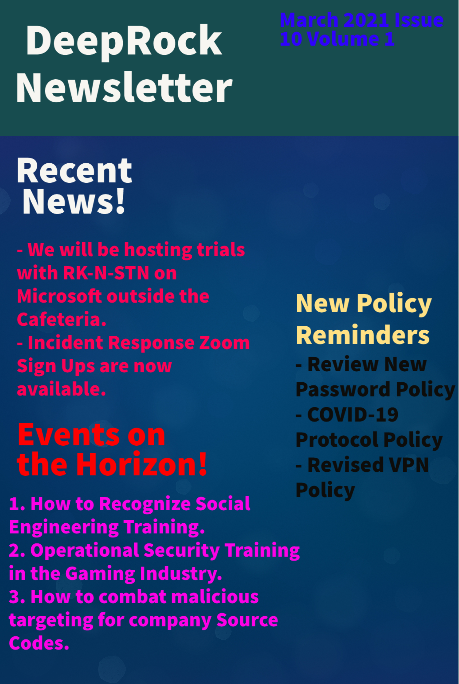
* One can go through training via a computer platform by going onto DeepRock’s developed website training gateway, this will include online assessments to certify understanding.
* There will be training for active on-site workers which will encompass how to best use DeepRock hardware and software in focus of their specific jobs and required everyday tasks.
* Web sessions and symposiums will also be of availability for any distance learners. This would allow new employee learners to choose and join programs concerning their suitable subject matter.
* There will also be onsite class instruction to teach practical abilities for the need for any specific product accreditation. Certified instructors will be stationed on DeepRock grounds that will run a class of personnel on specific topics.

DeepRock’s teaching department are accountable for the formation and allocation of the stated curriculum-based approaches for personnel, suppliers, and business shareholders who operate any of DeepRock’s customer services. These endeavors will be shared with the Information Technology sector if there is any requirement to deliver substances by electronic means or via DeepRock’s website training gateway.

Security training platforms and operations will be organized every four months to maintain personnel’s security consciousness. This will be a requirement for all personnel, there will be no exemptions to not take the training course because of the availability it has online. Moreover, if one were to fail in completing the security curricula or received inadequate outcomes with their assessment grades, they will be evaluated by DeepRock’s supervision unit to better understand the situation.

Finally, success of this developed training program will be evaluated through the use of gathered responses from personnel, which will be anonymous, however their company division will be known. The perception that DeepRock employees give is crucial to recognizing this teaching platform's efficacy and the system of measurement that will be gathered concerning the achievement of security training operations.

**Security Newsletter**

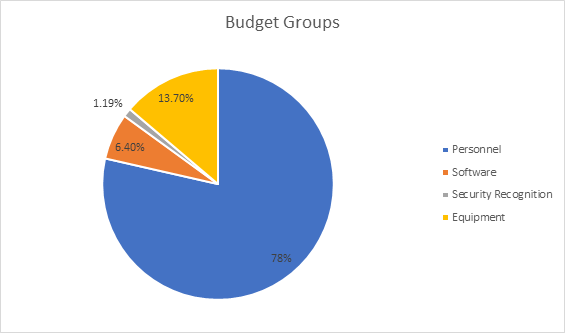
The final part of DeepRock’s security awareness instruction is a company developed newsletter that is issued monthly either through email or physically in employee mailboxes. DeepRock’s cybersecurity unit delivers these newsletters to each person that has a DeepRock email or mailbox account. The newsletter contains important features that help individuals become aware of cybersecurity specialists and highly regarded informational sources. We have copied one of DeepRock’s newsletters below to display an example. 

**Budget**

We have developed a thorough economic report as a part of our strategic plan. DeepRock’s distinguished budget identifies what assets will be obtainable by the company. What is also demonstrated is an analysis of the financial distribution within the department of information security found at DeepRock. Four main groups of our budget were pinpointed, and we have displayed their place on the budget table and pie chart.

| **Budget Group** | **Report** |
| --- | --- |
| **Personnel** | This group consists of company instruction, benefits, and wages for all security personnel. |
| **Software** | Group consists of endpoint security and supervising resolution programs and protective devices utilized to recognize, register, and mitigate any defense concerns. |
| **Security Recognition** | This group consists of the associated costs necessary for the illustrated educational security courses, plus the company newsletter. |
| **Equipment** | Group consists of protective tools and physical monitors, for example, locks which utilize biometric configurations and access cards. These are utilized to safeguard DeepRock’s physical sites. The repairs involved with all DeepRock systems are incorporated. |

| **Element** | **Fiscal Sum** |
| --- | --- |
| **Personnel:**· Company Instruction· Benefits· Wages | **$2,300,000** |
| $60,000 |
| $600,000 |
| $1,640,000 |
| **Software:**· Endpoint Security· Supervising Resolution Programs· Protective Devices | **$190,000** |
| $90,000 |
| $60,000 |
| $40,000 |
| **Security Recognition:**· Educational Security Courses· Company Newsletter | **$35,000** |
| $30,000 |
| $5,000 |
| **Equipment:**· Protective Tools· Physical Monitors and Appliances· Repairs & Replacements | **$400,000** |
| $20,000 |
| $340,000 |
| $40,000 |
| **Total Amount** | **$2,925,000** |



Our complete recommended budget comes out at $2,925,000. Our personnel take up a large portion of the budget allocation. This consists of enrolling strong ability with elevated salary and benefits, preparing them appropriately, including retaining these workers to hold up the substantial scope of DeepRock’s security division. The equipment resources section of our budget consists of supervising DeepRock’s technological foundation stretching across countries and continents with the gaming and social media platform. The smaller portions of the allocated budget is for software and security recognition for employees. This is put in place to guarantee that DeepRock is resistant to data security incidents through fostering security consciousness and engaging courses that examine and detect any questionable security matters.

**Executive Summary**

Some time ago, data protection was naturally deemed a buried expense for numerous companies, granted that their information had never been infringed: yet. Nonetheless, the modern high frequency of constant attacks in the cyber realm for companies all around the globe and the growing risk environment has resulted in breached information and broken businesses. To make matters worse for companies without data security, these incidents are including serious penalties for compliance and privacy policy violations. The value of promoting the infosec department and their necessity for an organization is essential for success in company confidentiality.

Therefore, in arrangement with the presented situation and DeepRock’s international prominence in gaming and social media data, information security linking to efficient use of security tools to grow in proficiency, personnel engagement, and competitive advantage has been merged into DeepRock’s planned strategic cybersecurity management strategy.

The constructed strategic cybersecurity management plan for DeepRock looks to preserve our company’s security and attentiveness for any potential cybersecurity incidents that could occur. In addition, it has been constructed to guarantee that key company processes will remain, even when unexpected experiences or disasters take place. Accordingly, with the aim of accomplishing these objectives, a frequent backing from DeepRock’s executive unit will be necessary in order to account for the deliberated main parts. This includes the key group of forming a security-conscious and seasoned personnel and retaining personnel for the substantial scope of DeepRock’s robust defense sector.

**References**

Baskerville, S. (2017). Security metrics – reasons why you should measure them. Retrieved from: [Here](https://www.proserveit.com/blog/security-metrics-program#:~:text=Metrics%20help%20to%20continually%20prove%20security%27s%20worth&text=This%20trend%20allows%20the%20security,on%20the%20organization%27s%20risk%20tolerance)

Gulati, R. (2003). The threat of social engineering and your defense against it. *SANS Reading Room,* Retrieved from: [Here](https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.800.4413&rep=rep1&type=pdf)

Infotech, N. (2021). Security practices in game design and development. Retrieved from: [Here](https://trcstaffing.com/blog-how-many-rounds-of-interviews-are-too-many/#:~:text=While%20there%20is%20no%20hard,position%2C%20is%20a%20wise%20move)

IP, E. (2018). 4 benefits of disaster recovery planning. Retrieved from: [Here](https://www.evolveip.net/blog/4-benefits-disaster-recovery-planning)

Kumar, A., Chaudhary, M., & Kumar, N. (2015). Social engineering threats and awareness: A survey. *European Journal of Advances in Engineering and Technology, 2*(11), 15-19. Retrieved from: [Here](https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1075.1678&rep=rep1&type=pdf)

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST Special Publication, 800*(2017), 181. Retrieved from: [Here](https://scadahacker.com/library/Documents/Frameworks/NIST%20-%20800-181%20-%20NICE%20Cybersecurity%20Workforce%20Framework.pdf)

Nibusinessinfo. (2021). Business continuity and crisis management: Advantages of business continuity planning. Retrieved from: [Here](https://www.nibusinessinfo.co.uk/content/advantages-business-continuity-planning)

TerranovaSecurity. (2021). How to build a strong security awareness program in 2021 . Retrieved from: [Here](https://terranovasecurity.com/how-to-build-a-strong-security-awareness-program-in-2021/)

TrcStaffing. (2021). How many rounds of interviews are too many?. Retrieved from: [Here](https://trcstaffing.com/blog-how-many-rounds-of-interviews-are-too-many/#:~:text=While%20there%20is%20no%20hard,position%2C%20is%20a%20wise%20move)

Zippia. (2021). Working as a security technician. Retrieved from: [Here](https://www.zippia.com/security-technician-jobs/)