**BlackRock INC. Strategic Cybersecurity Plan (II)**

**By**

**Natnael kebede**

**University of Dallas**

**2020**

This Paper Submitted in Partial Fulfillment of the Requirements for

CYBS 8396 – Strategic Cybersecurity Practicum

Summer 2020

Presented to Professor Brian Wrozek

# **Table of Contents**

[Introduction 3](#_Toc46778363)

[Security Metrics 4](#_Toc46778364)

[Business Continuity Strategy 7](#_Toc46778365)

[Disaster Recovery Plan 9](#_Toc46778366)

[Security Staffing Strategy 11](#_Toc46778367)

[Security Position Job Posting 14](#_Toc46778368)

[Security Awareness Plan 16](#_Toc46778369)

[Security Newsletter 18](#_Toc46778370)

[Budget 19](#_Toc46778371)

[Executive Summary 20](#_Toc46778372)

[References 22](#_Toc46778373)

# Introduction

BlackRock Incorporated is a global leader in investment, risk management, advisory, and technology solutions that helps investors build better financial futures. We are also a leader in asset management with $14.2 billion in total revenues in FY 2018 and $6.5 trillion in managed assets as of the first quarter of 2019 (“Introduction to BlackRock”, n.d.). Throughout our 32 years of existence, we have always put our clients first, acted on their behalf as trustees, and have seen circumstances through their eyes to deliver exceptional investment platforms and services.

We also understand their concerns in protecting their personal information that we collect and share to run our daily functions, depending on the products or services they have with us. As a result, we have pushed information security to the forefront of the organization’s plan in today’s threat-filled landscape.

That said, this document is drafted to complete a two-part strategic cybersecurity management plan for BlackRock with the aim of keeping the organization secure and prepared for any incidences that may arise in the realm of information security. The plan begins with security metrics that will be used to measure the effectiveness of the information security program within the company by targeting expense related processes to maximize performance in alignment with BlackRock’s business values (“BlackRock Mission, Vision & Values”, n.d.).Following that, the topics of business continuity and disaster recovery are addressed as it relates to a security incident, with a sample guideline outlined for a given emergency or disaster scenario. Subsequently, the crucial process of staffing an information security team for the company is addressed, along with a sample job posting for a security position. Finally, the ever-important topic of security education is discussed with suggested themes and topics to be covered. A sample newsletter is also provided to keep employees’ security awareness updated.

Aligned with the leadership team’s approval, this two-part strategic cybersecurity plan is recommended for adoption. Its purpose will be to guide the security operations within BlackRock and serve as a strong foundation to build upon for creating comprehensive and detailed cybersecurity procedures for the company.

*Natnael M. Kebede*

Managing Director and CISO.

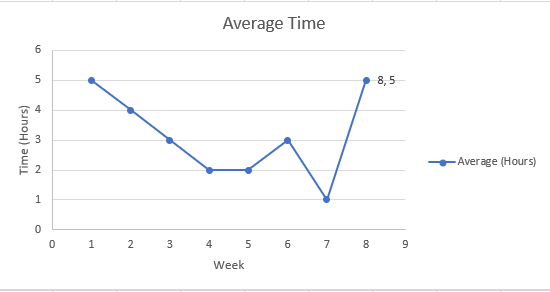
# Security Metrics

To ensure that a proposed plan is effective, goals and security measurements must be defined so that they can be tracked and reported upon. This is possible through the use of security matrices, which provide valuable information on the performance of the cybersecurity team and help leaders make appropriate risk trade-off decisions. The following consists of the metrics associated with this plan that will measure the effectiveness of the proposed cybersecurity management plan for BlackRock.

**1) Time to Access Resources:** One of the security-related measurements that will be tracked and reported at BlackRock is the time it takes for users (clients, employees, and stakeholders) to reset their password to access their respective investment management service accounts, as well as shared IT services within the organization such as Active Directory or Lightweight Directory Access Protocol.

This metric is collected due to the sunk cost in productivity that occurs when they are locked out of their account. That is, once locked, end-users will not be able to complete transactions (for clients), and tasks (for employees), which in turn affects the bottom-line of the company as some degree of financial loss occurs lost every time they wait to get their access restored.

The metric will be used to track and improve the password reset process and to provide insights about the value of executing this security function through reduced time, thereby lowering productivity and financial loss. The audience for this metric will be the Help Desk Support lead, System Administrators, Director of Infrastructure Security, and the Identity Access Management Manager so that they can suggest effective strategies on where improvements can be made. This metric shall be collected weekly and presented every two months. The responsibility for collecting, analyzing, and reporting will be handled by Identity Access Management (IAM) specialists, in collaboration with Help Desk Technicians. This security metric is visualized, as shown in the screen capture below.

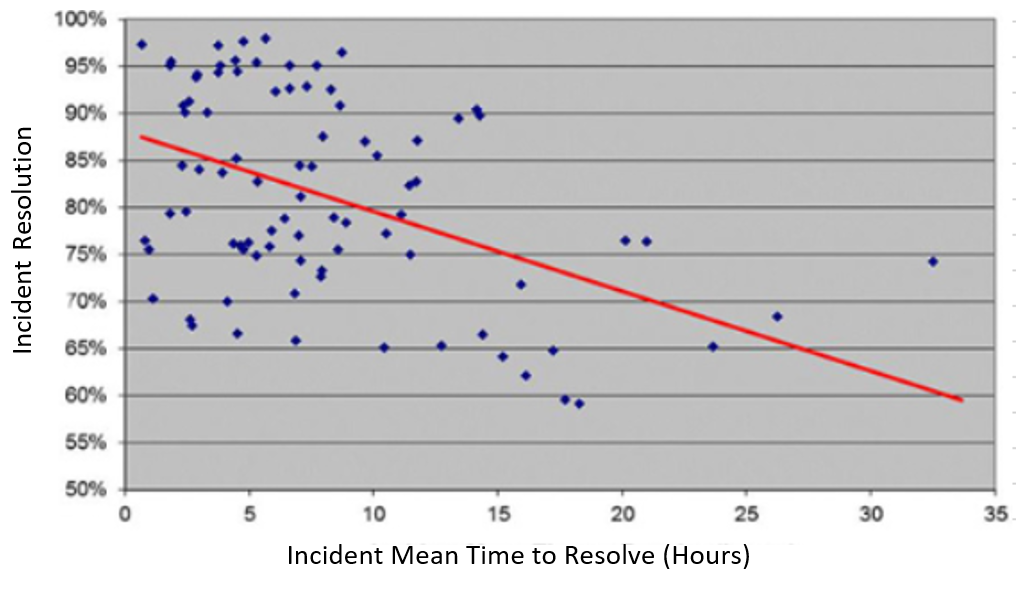


**2) Time to Remediate Incidents:** The second security metric that will be tracked and reported is the time it takes to remediate security incidences related to company desktops. As a valued asset within the company, desktops, and laptops are often used by staff members to interact with critical assets such as internal networks and servers, as well as confidential data.

This metric is carefully collected to serve as an indicator of the value of BlackRock's information security program. It is also a component whose prolonged nature increases the risk value of desktops and laptops as an asset.

The metric will be used to track and improve the remediation process of security incidents for these devices. Additionally, it will be utilized to express the security awareness of staff members as well as any productivity and financial loss that might be incurred as a result of security incidents with these devices (Hayslip, 2018).

The audience for this metric will be the Head of Incident Response and the Enterprise Support Lead, as they work together to remediate the desktop security incidences. This metric shall be collected hourly and presented every month. Security Analysts and Senior Incident Responders will handle the responsibility for collecting, analyzing, and reporting. This security metric is visualized, as shown in the screen capture below.



**3) Security Awareness Rate:** The third security metric that will be tracked and reported is the completion rate of security awareness campaigns. This metric is carefully collected to serve as an indicator of the security awareness posture of BlackRock from a social engineering perspective. It also serves as a useful tool for auditing purposes by aiding the leadership team to analyze the organization's compliance regarding regularly scheduled staff training.

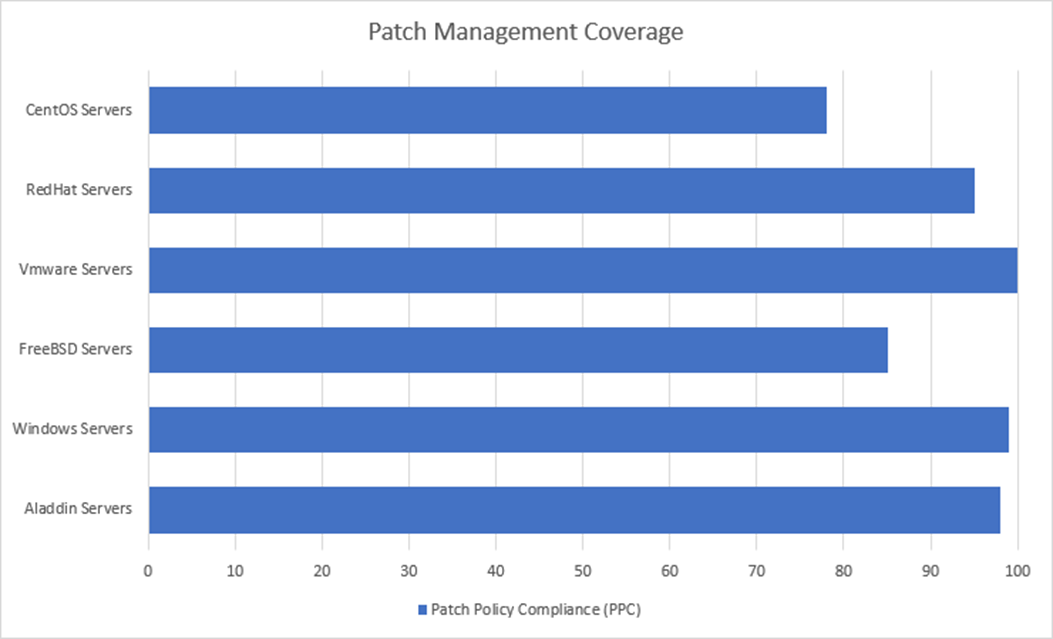
Additionally, this metric will be used to measure the effectiveness of security awareness campaigns and helps to identify areas of improvement, such as administering challenging assessments or utilizing different approaches to collect the performance of employees in their security understanding efforts.

The audience for this metric will be the Internal Chief Information Security Officer (CISO). This metric shall be collected based on the frequency at which the awareness campaigns are carried out. The metric will be reported four times a year or every three months. The responsibility for collecting, analyzing, and reporting will be handled by the Senior Program Manager of Global Education, who works closely with the training division. This security metric is visualized, as shown in the screen capture below.



**4) Patch Management Coverage:** The fourth security metric that shall be tracked and reported is the patch policy compliance of servers. This metric is collected weekly and reported every month. This metric is useful as it shows the organization's risk posture and helps in tracking the vulnerabilities that exist on critical corporate servers. Additionally, it will serve as a good indicator of the compliance level that the servers are-in when compared to BlackRock’s patch policy. The metric will be calculated by comparing the number of fully compliant servers to the patch policy against all servers under patch management. The result is then represented as an integer value with a range of 0 -100.

This metric will be used to understand BlackRock’s patch management program's effectiveness. It also helps to identify areas for improvement, including areas where more resources would need to be allocated. This technique will help during audits and compliance checks by proving that the company is compliant with applicable standards and laws. Moreover, the metric can show the organization’s risk acceptance decisions regarding patch management. The audience for this metric shall be the Business System Analysts, Server Administrators, Director of Infrastructure Security, Senior Director of Security Operations, and representatives from and the risk and compliance team. The responsibility for collecting, analyzing, and reporting will be handled by the vulnerability management who monitor asset tracking and vulnerability scanning tools. This security metric is visualized, as shown in the screen capture below.



# Business Continuity Strategy

BlackRock relies on advanced information technology systems to meet daily business operations as well as power asset management services and products. The primary purpose of such systems within BlackRock is to create exceptional financial future outcomes for customers by connecting them to essential services and thereby leading the digitalization of managing investments regardless of the geographical location (E., 2017). However, in the information security space, anything that can go wrong will go wrong. Nothing is 100% guaranteed to be available all the time. Hence, as part of this strategic cybersecurity management plan, a business continuity strategy plan is incorporated for BlackRock to use if a disaster is so profound that business operations cannot continue as usual.

The CEO and COO of BlackRock will manage the Business Continuity Plan (BCP). It will be put into action concurrently with disaster recovery procedures taking place. The plan's primary goal is to ensure that critical business operations will continue even when unplanned events or emergencies occur. The plan will be achieved via various components discussed below.

First, the continuity strategy to be used is a hot site. In this off-premise location, the company’s work can resume during an emergency or disaster. The site is hosted with all the necessary equipment necessary, including backup data, computers, phones, and related peripherals for the business to continue (Swanson, et al., 2010). The site is crucial for BlackRock during such events due to the organization’s time-sensitive nature of operations and services. Even half an hour of downtime can be disastrous since investors using BlackRock’s services lose visibility of their assets and the ability to perform trades, which in the world of investment can lead to the loss of a favorable financial position. Hence, high availability and redundancy shall be built into the hot site, with fully redundant systems that are load-balanced and exhibiting bi-hourly data mirroring and data replication.

The business continuity strategy will be applied to the highest value assets such as employees, Aladdin Operating System (OS), applications, databases, web servers, peripherals and phone systems, and workstations. It is also applicable to computing resources such as networks (both physical and virtual) and other vital services, which were all identified in the risk assessment document. These assets are involved in providing investment management services that form the majority of BlackRock’s business and maintain the way operations are conducted. A summary of the critical operations that are in scope for business continuity is summarized in the table below.

|  |  |
| --- | --- |
| **Business Activity** | **Details** |
| On-site Support for Clients | Critical workflow to continue providing services and meet Service Level Agreement (SLA) requirements. |
| Technology Services Support (internal to BlackRock) | Incident response management.  Enterprise risk and regulatory advisory.  HR Payroll systems support for employee salaries.  Servicing of current computing resources.  Continued installation of new tools and applications.  Performing upgrades on current systems. |
| Communications | E-mail and social media support of customers and staff to maintain operations and keep them updated.  Communication support to resolve issues by reaching technicians. |
| Establishing a Failover Environment | Mapping network, hardware, and software to be used to achieve the minimum requirements for critical business operations.  Full replication and imaging of hot site computer resources to allow for immediate failover and minimum downtime in the event of a disaster. |

On the other hand, the following functions are deemed non-critical operations. They hence are out of scope for business continuity.

New application development and testing.

Support for non-critical applications such as employee training portals.

Sales operations pertaining to acquiring new clients.

Recruitment functions performed by Human Resources.

Furthermore, the key organizational players in implementing the business continuity strategy are summarized in the table below.

|  |  |
| --- | --- |
| **Roles** | **Responsibilities** |
| Chief Executive Officer (CEO) | Plays a crucial role in the decision making and communication processes of the BCP, including briefing senior management and the Executive Board on interruption events and recovery duration. The individual is also responsible for ensuring that the recovery team has the resources and support necessary to do its job. |
| Chief Operating Officer (COO) | Confirms critical business processes, services, employee roles, and technology are available to resume operations. |
| Chief Technology Officer (CTO) | Handles the overall responsibility of BlackRock’s information systems. |
| Managers | In charge of supervising business operations that rely on information systems. |
| Information security engineering and related staff | Responsible for the security activities involved in developing, implementing, and maintaining information systems. |
| Employees and Recovery Teams | Responsible for executing their assigned job functions and duties in the critical business operation areas. |

Finally, the BCP will be tested three times a year using a desk check exercise where the assigned duties and appropriate plans will be distributed to identified individuals within the organization. In this process, a walk-through of the plan is conducted to test whether the procedures will work as intended while also investigating any assumptions and highlighting gaps. Additionally, a simulation exercise (including tabletop) is to be carried out every year, where a role-playing exercise is carried out as though the actual disaster has occurred. The alternative site, including evacuation and communication, is also tested for operation capability (Grance et al., 2006). The test results will be used to present a report on the exercises, along with a proposed future exercise schedule, to senior management and board of directors. It might also be used to update the plan as appropriate.

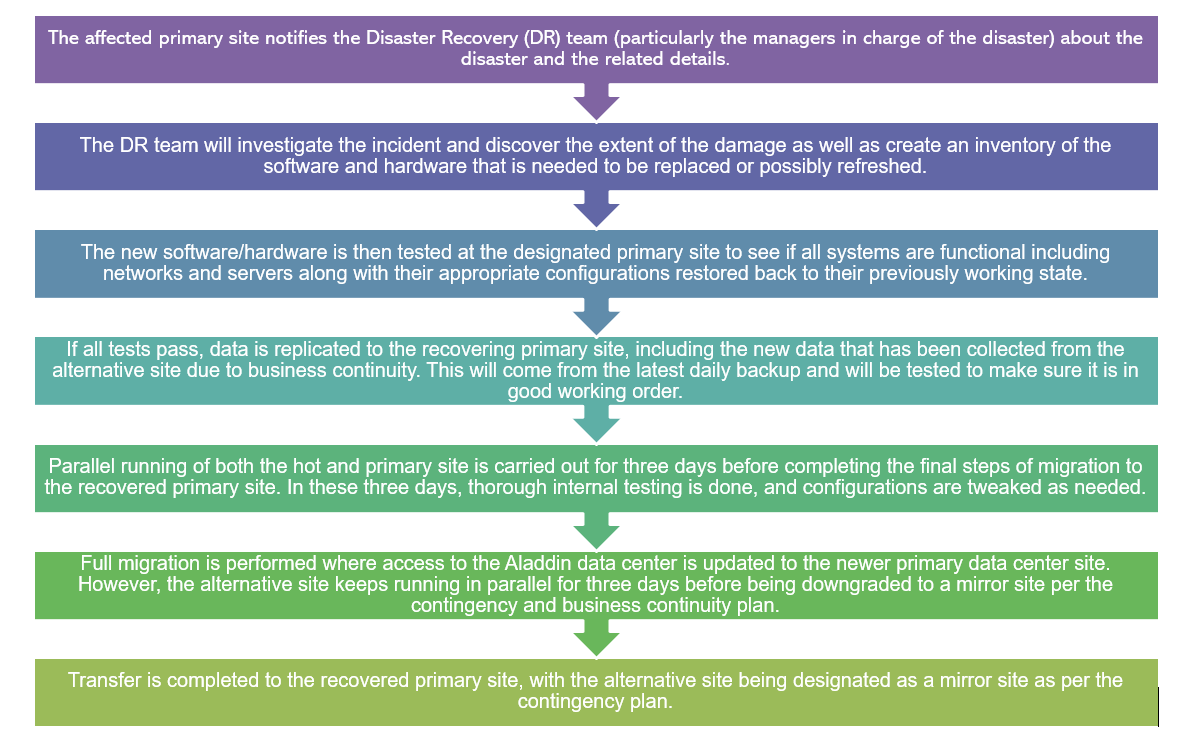
# Disaster Recovery Plan

Closely related to business continuity, disaster recovery plays a critical role in getting the entire business back to full functionality after a crisis. The preparation for disasters can be considered in action, for example, by examining the recovery of the data center that runs BlackRock’s Aladdin Operating System, a high-value asset as identified in the organization’s risk assessment document. The asset is used to manage investments by considering the market conditions, news, weather, people, and technology to analyze risk and manage the associated money strategically in real-time. Hence, it provides a significant profit source and contains sensitive information used in transactions such as credit card numbers and social security numbers for enrollment.

Some of the primary actions that should have been taken before recovering the Operating System’s data center are:

* The aim is to make the service offering available to clients and not for other aspects such as software development or testing.
* A business continuity plan is already in effect, with the alternative hot site ready.
* The source code and databases of activities performed within Aladdin OS are backed up every night to the hot site, ready to go live in a moment’s notice.
* A live mirroring of the services, installed applications, and database used in the system is mirrored to an AWS (Amazon Web Services) cloud storage offering.

Following the above action plans, the Data Center team, including the Application Server Administrators, Database Administrator, and a Network Administrator, will perform the recovery. Their respective managers or leads will lead the restoration with the direction of the CIO and Director of Enterprise Services. The following chart displays the list of procedures to be executed in recovering the Aladdin OS’ data center.



# Security Staffing Strategy

Like any organization, being able to attract, recruit, and retain talent is critical for BlackRock's existence and success. Hence, as part of this strategic cybersecurity management plan, a security staffing strategy is incorporated for the company to utilize in addressing the vital and sensitive process of recruiting, hiring, managing, and terminating employees. The following table summarizes the various ways the organization will acquire new hires.

|  |  |
| --- | --- |
| Means of Hiring | Description |
| Internal Job Application Portal | New hires scouted through this process are current employees. They have gone through the hiring process at least once and were deemed to be a fit for BlackRock. |
| Employee Referrals | Due to the in-depth knowledge of the company’s culture and operations, employees would likely be able to identify suitable candidates for various job roles. Such employees must first attest to the organization’s anti-corruption policy in the recommendation process, which stipulates that they do not give recommendations for jobs and roles in a nepotistic manner. |
| BlackRock’s Public Job Portal | Candidates can apply for the roles they think they are fit for online. Once they submit their application, the recruitment team will review before moving forward in the recruitment process. |
| Online Job Boards | BlackRock accepts applicants through LinkedIn, Indeed, Glassdoor, and Dice. These boards will provide access to a vast pool of candidates that the recruitment team will review before moving forward in the recruitment process. |
| Staffing Agencies | Staffing agencies perform screening activities and try to match candidates to the organization’s open roles. However, they are considered the least means in looking for candidates due to the associated costs of recruiting candidates. |

The security team primarily looks for technical skills. Such skills are the most crucial as they are the skills needed to get the job done and reduce the training requirements needed to get a chosen candidate up-to-speed. As a result, a baseline of education and certifications are required per the DoD 8570.01’s Manual: Information Assurance Technical Level II (Grimes, 2015). This requirement includes CompTIA Security Analyst+ and Systems Security Certified Practitioner, among many others, with the additional requirement of Computer Networking proficiency. Such skills can also be supplemented with a formal degree from an accredited institution, with a baseline being a bachelor’s degree in the field of Information Technology (IT), focusing on an area of cybersecurity.

The above skills are followed by soft skills such as effective communication and presentation. Such skills are essential since working in the security team involves collaborating with various personalities and skillsets, with some staff members being not as technically adept as the security and IT specialists. Additionally, BlackRock’s business requires much liaising with clients and business specialists. Hence, having excellent communication and presentation skills is essential to explain technical details to managers, directors, and the executive team as well to work together with other team members and clients.

In terms of the interviewing and on-boarding process to attract the above skills, the following table summarizes the procedures to be followed.

|  |  |
| --- | --- |
| Interview Process | Description |
| Initial Phone/Video Interview | Candidates will primarily get screened via a call to gauge their interest in the role they applied for and to simplify verify that they meet the minimum requirements of the job per their Resume and Cover Letter |
| Second Interview | Upon passing the initial screening, the candidate will be evaluated for their technical skills, professionalism, and ability to communicate with interviewers and express themselves. The interview will also help determine whether the candidate’s career interests align with the organization and the team’s needs in the near long-term. |
| Third Round of Interviews | Upon confirming that the candidate has the soft skills and that their career interests align with the company’s needs, this interview is conducted by technical leads and managers to determine if the candidate will be able to carry out the role-specific duties required. |

If the candidate the screening and interview steps of the recruitment process and is deemed to be the best fit for the organization and role in the security team, an official job offer letter is emailed to the individual with a timeline to respond. If the person accepts before the cutoff date instructed, the on-boarding process begins with a list of next steps communicated by the HR team. Some of this includes submitting background check and credit information. The individual will also be required to sign a non-disclosure agreement (NDA) and comply with a few company policies.

Furthermore, top talent will be attracted to BlackRock by offering benefits such as:

* Providing competitive salaries compared to similar roles in other organizations.
* Higher than the average matching of 401(k) plan, given BlackRock’s investment expertise.
* Education reimbursement programs, pet, and health insurance, and 24/7 access to a fitness center.
* Paid time off, such as PTO, sick days, and vacation days.

Once candidates are on-boarded, in addition to shadowing fellow peers to get them up to speed on performing their duties, they will be trained through various means. Some ways include the company’s training portal, where HR and their managers can assign them materials to complete, and through online learning platforms, the company has premium subscriptions to. Some of these include O’Reilly, Udemy, Linux Academy, and LinkedIn Learning. Other free resources provided by Sans, Cybrary and the U.S Department of Homeland Security can also be recommended for appropriate training purposes.

To maintain these new security employees for the long term, the following retention strategy will be used.

* Unique offerings such as industry certificate maintenance programs, advanced security training, and attendance of security conferences for free, such as attending AWS re: Invent, SANS Hackfest, and Blackhat USA.
* Two days per week work from home offering after a year of working from the office.
* Rotational three-day weekends, every two months, the IT Security staff will be offered a paid Friday off for at least a quarter of the team.
* Internal promotions where applicable to give new employees more confidence in their job assessment and growth track.
* Substantial bonus of 3% after working for 1-2 years. This rate can be up to 6% for good financial years to signify that employees' work is being appreciated.
* Substantial bonus of 6% at the end of good financial years. This will be a rate that is intended to be higher than average and will keep the employees happy knowing that their work is being appreciated.

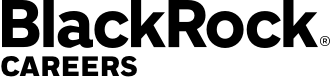
Finally, in the instance that a security personnel leaves the company, the security staffing strategy will also be used to address the vital and sensitive process involved in the off-boarding of employees. As a result, the following procedures are recommended as a guide for handling such situations.

* The employee’s manager, IT team, and HR should be notified about the employee’s leave. Depending on friendly or harsh off-boarding, the individual’s access to corporate resources will be terminated before or as soon as the notification for leaving occurs.
* The employee will be required to return company properties such as a badge, laptop, media, physical access controls (access card or keys), and paper documents or data. The leaving employee’s computer hard drive should also be secured (Wheatley, 2003).
* Physical locks to the leaving employee’s office and storage areas should be changed.
* The employee’s personal belongings should be removed from the company’s premises.

Once these steps are checked and verified appropriately, the leaving employee should then be escorted from the building by security guards.

# Security Position Job Posting

A sample job description in alignment with the security staffing strategy described above is detailed below. As depicted in the advertisement, instead of mentioning specific applications and technologies utilized at BlackRock, the skills required to perform the duties of the role are provided. The sample posting pertains to a Level One Security Analyst position.

 (BlackRock Incorporated, n.d.).

Overview

Job Title: Security Analyst I  
Reports To: Security Operations Center Team Lead

Location: Atlanta, Georgia, US

Team: Global Security Office (GSO)

Job ID: 0104347

Posting Date: 7/25/2020

Position Description

The Security Analyst I role entails providing vulnerability and threat analysis and monitoring of logs for a large number of information systems. Additionally, the individual will be responsible for analyzing, responding, and investigating hardware and software vulnerabilities.

Qualifications and Required Skills

* A Bachelor’s degree from an accredited institution with cybersecurity concentration or an equivalent amount of education and experience.
* 1-3 years of experience in cybersecurity functions such as Incident Response or related position, preferably in the financial services industry.
* Hands-on experience with Windows/Linux systems and security tools such as IDSs, Firewalls, SIEMs.
* Knowledge of basic networking protocols and services (SSH, TCP/IP, DNS, FTP, DHCP, etc.)
* Experience with one or more of the following scripting languages: SQL, Java, Python
* Related IT Security certifications (Security+, CCNA, Network+, CySA+, or equivalent) are considered a plus.
* Detail-oriented, able to multi-task and prioritize in a fast-paced environment.
* Excellent listening and communication skills, both written and verbal.
* Self-starter, with strong initiative.

Responsibilities

* Analyze log files from various sources (e.g., host logs, intrusion detection system logs, firewall logs, and network traffic logs) to identify possible threats to network security.
* Receive and analyze alerts from various sources to determine the root cause of such alerts.
* Track and document cyber defense incidents from initial detection through final resolution.
* Perform malware analysis on malicious files to gather indicators of compromise.
* Perform log analysis within a log aggregator to timeline an event.
* Perform a collection of forensic artifacts and inspect to discern possible mitigation/remediation.
* Coordinate with intelligence analysts to correlate threat assessment data.

How to Apply

Please apply to this job via the BlackRock career portal using the associated Job ID at <https://careers.blackrock.com>

About BlackRock

As a truly global organization, BlackRock combines the advantages of a worldwide reach with local relationships and services. This allows us to manage assets for customers across the 7 main continents, employ an estimated 14,900 skilled professionals, and have offices in 30+ countries worldwide. We are one of the world's leading solution providers in risk management, advisory, and investment. Our solutions range from essential and measurable active management methods that maximize performance to well-optimized indexing plans created to achieve comprehensive exposure to world capital markets.

Throughout our 32 years of existence, we have always put our clients first. Their needs are of the highest importance, and we act on their behalf as trustees. Our team’s investment approach is based on the belief that we are capable of gathering market insights and utilizing global reach and devotion, focusing on risk management to deliver exceptional performance in all market environments. As such, we aim to be the best in achieving a balance between opportunity and risk (BlackRock Incorporated, 2019).

# Security Awareness Plan

One of the most important ways to establish and maintain security practices within an organization is to educate employees and maintain their awareness of information security components. Hence, as part of this strategic cybersecurity management plan, a security staffing awareness plan is incorporated for BlackRock to utilize and help employees understand their roles and responsibilities related to cybersecurity.

The security education and awareness program's elements will consist of the following three main aspects that host the diverse content within the delivered training.

1. **General User Training:** This training consists of content that will apply to all employees and contractors. It covers topics such as data protection, managing passwords, best practices when executing job duties, and procedures to follow when reporting security violations.
2. **Managerial Training:** This training targets managers and covers information such as handling specialized access control, security issues in permitting access to resources, and making the right management decisions.
3. **Technical Training:** This training is tailored to staff members, such as IT specialists, system administrators, and security professionals. It covers advanced technical content as applicable to their complex responsibilities. It also details technical information regarding the tools they utilize or administer. Some of these include Deep Security, Veracode, Alert Logic, Nexpose Vulnerability Scanner, QRadar, and Microsoft SQL Server, and many others.

That said, the various key themes and topics to be covered by the security awareness program include:

1. **Online Behavior Theme:** In this topic, employees will be educated on how to use the internet and networks appropriately to access corporate resources. This includes avoiding spoofed networks, the importance of connecting to BlackRock’s Virtual Private Network (VPN), strong password practices, and regularly updating operating system software and applications.
2. **Social Engineering Theme**: In this topic, employees will be educated to recognize and mitigate social engineering techniques. This includes identifying phishing emails and physical security problems such as shoulder surfing and tailgating. The topic aims to keep attackers at bay with a workforce that is mindful of what is happening around them and recognize suspicious behavior both physically and electronically, allowing them to alert the respective teams to deal with the security issue (Dempsey, Nieles & Pillitteri, 2017).
3. **Malware Theme:** In this topic, employees will be educated to recognize malware and the damage it can bring to data and application software. This includes understanding the behaviors of viruses, avoiding ransomware, the importance of regularly scheduled data backups and virus scans, identifying secure and legitimate sites, and avoiding downloads from places other than BlackRock’s software center.
4. **Data Protection Theme:** In this topic, employees will be educated on data security and privacy, the classifications of corporate data, and how to handle data appropriately when working with clients. This includes storing data on company-approved systems, protecting unauthorized access to stored information, and regulations such as the General Data Protection Regulation (GDPR) that BlackRock abides by, including the consequence of legal fines for leaked data.

Altogether, the security training and awareness elements, including the themes and topics above, shall be communicated using the following techniques:

* Computer-based training through BlackRock’s training portal.
* Practical on the job training about the use of hardware, software, and procedures, as needed to perform their job duties.
* Web seminars and distance learning, where trainees attend a course regarding the appropriate topic.
* Formal in-class training to educate technical skills such as for product certification purposes. In such a communication format, a trainer located on-site will lead a group of employees on a given subject.
* Publicly visible and available posters around the building and additional reminder content and campaigns are delivered via email.

The training division, reporting to the Senior Program Manager of Global Education, is responsible for the creation and distribution of the above communication strategies to employees, contractors, and company stakeholders who utilize the organization’s services. Such efforts will be communicated with the IT team if there is a need to distribute content electronically or through the organization’s training portal. The frequency for communication will be four times a year to remind them that appropriate resources are available for them to review.

On the other hand, security awareness programs and campaigns will be conducted every three months to keep the staff updated with their security awareness skills. No exemption will be provided to opt-out of such training. Additionally, failing to complete the training or unsatisfactory assessment results reviewed by the management team.

Lastly, the security education training and awareness program’s success will be measured by the collected feedback from employees. The insight they provide is key to understanding the program's effectiveness and the metrics that will be collected regarding the completion of security awareness campaigns, as described in the Security Awareness Rate section above.

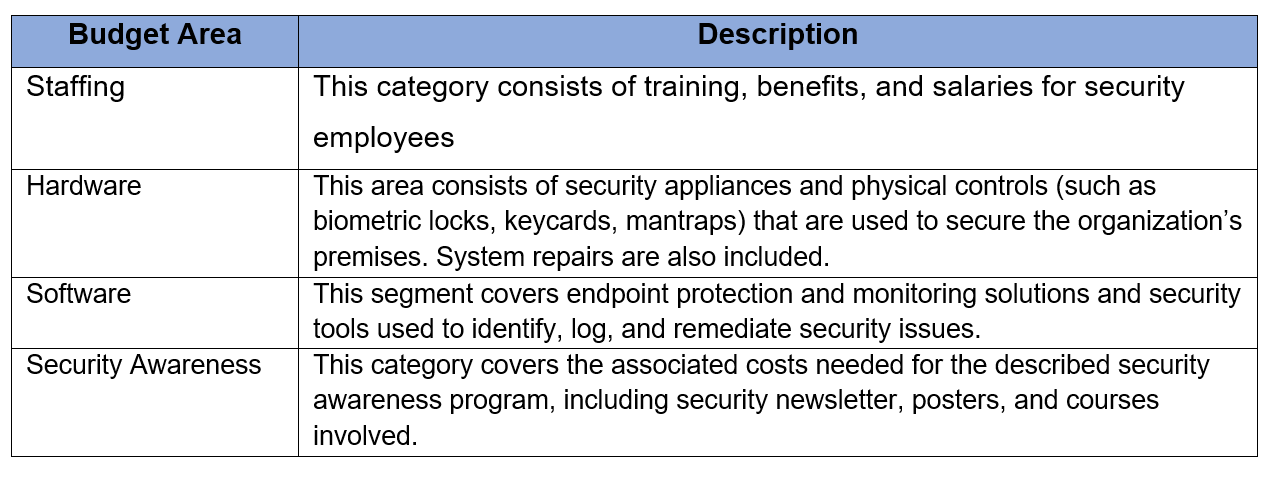
# Security Newsletter

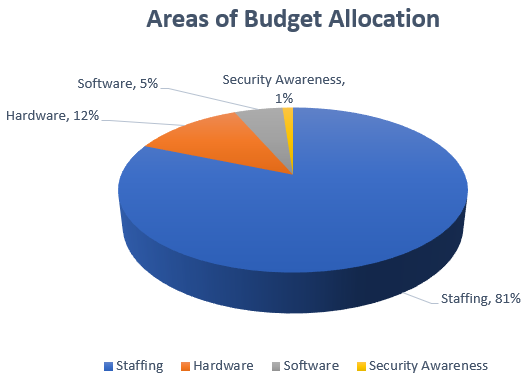
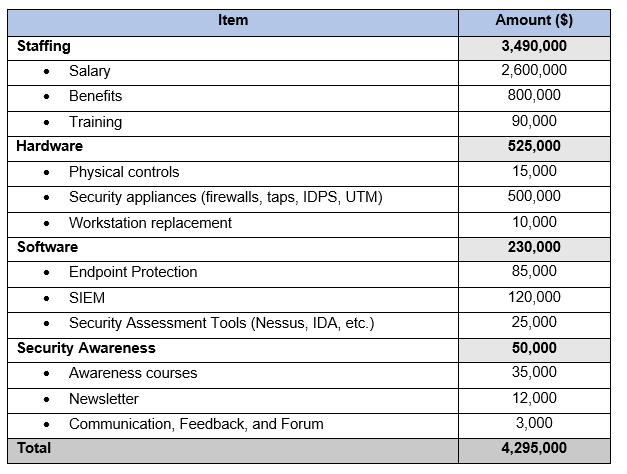
The last component of BlackRock’s security education training and awareness program is a newsletter distributed monthly via email. The security newsletter is sent out from the cybersecurity team’s mailbox on behalf of the CEO to all individuals with a BlackRock email account. The newsletter includes links and headlines that direct readers to articles written by well-known cybersecurity experts and reputable news sources. The details of the newsletter will be laid out, as shown in the image below.



# Budget

No plan is complete without a detailed budget to execute it. Hence, as part of this strategic cybersecurity management plan, a comprehensive financial information is included. The budget defines what resources can and cannot be available and shows a breakdown of the monetary allocation across the information security department. That is, in alignment with the strategic security plan, the following four key categories are identified, followed by their corresponding budget spreadsheet and chart.





As shown in the spreadsheet above, the total proposed budget is $4.295 Million. The reason for this high financial allocation emerges from 81% of the cost allocation set for staffing needs, such as recruiting for top talent through high pay and benefits, train them accordingly, as well as to maintain employees for the large size of the security department. The second-highest spending of 12% on hardware resources is proposed due to the need to monitor BlackRock’s technology infrastructure given the large scale of the organization’s global operations and investment portfolio of $6.5 trillion in managed assets (“Introduction to BlackRock”, n.d.). Finally, the lesser budget allocation for software and security awareness is still satisfactory to ensure that the organization is resilient to information security attacks by promoting mindfulness, inspiring individuals, and employing programs that monitor and identify security concerns.

# Executive Summary

In the past, information security was typically considered a sunken cost in many organizations, given that their data had not been breached yet. However, the recent prevalence of consistent cyber-attacks and the ever-changing threat landscape in the news today has resulted in leaked data and damaged reputation. Not to mention, it is followed by severe fines for violation compliance standards and privacy policies. Hence, the importance of pushing information security to the forefront of an organization’s priority list is crucial.

Hence, in alignment with this scenario and BlackRock’s global business activities, information security relating to the effective use of digital tools to increase productivity, efficiency, competitive advantage, employee engagement, and clients’ insights has been incorporated into the organization’s proposed strategic cybersecurity management plan.

The two-part strategic cybersecurity management plan for BlackRock aims to keep the organization secure and prepared for any incidences that may arise in the realm of information security as well as to ensure that critical business operations will continue even when unplanned events or emergencies occur. As a result, in order to achieve these goals, a continual support and funding are needed from the executive team to address the discussed key areas, including the principal category of establishing a security-aware well-rounded workforce and maintaining employees for the large size of the security department.

# References

BlackRock Incorporated. (n.d.). Blackrock-careers\_logo\_black.png (330×78) [Image]. Retrieved from https://cdn-static.findly.com/wp-content/uploads/sites/937/2019/07/blackrock-careers\_logo\_black.png

BlackRock Incorporated. (2019). *2019 Annual Report*. Retrieved from https://s24.q4cdn.com/856567660/files/doc\_financials/2019/ar/BlackRock-2019-Annual-Report.pdf

BlackRock Mission, Vision & Values. (n.d.). Retrieved from https://www.comparably.com/companies/blackrock/mission

Dempsey, Nieles, Pillitteri. (2017). NIST Special Publication 800-12 Revision 1. *An introduction to Information Security*. Retrieved from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

E. (2017). Between a Rock and a Hard Place: How BlackRock is Winning the War on Technology – Technology and Operations Management. *Harvard Business School.* Retrieved from https://rctom.hbs.org/submission/between-a-rock-and-a-hard-place-how-blackrock-is-winning-the-war-on-technology/

Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., & Good, T. (2006). *Guide to test, training, and exercise programs for IT plans and capabilities* (No. NIST SP 800-84). https://doi.org/10.6028/NIST.SP.800-84

Grimes, J. (2015). *Information Assurance Workforce Improvement Program* (DoD 8570.01-M). Retrieved from https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf

Hayslip, G. (2018). Security metrics: Telling your Value Story. Retrieved from CSO Online website: https://www.csoonline.com/article/3253332/security-metrics-telling-your-value-story.html

Introduction to BlackRock. (n.d.). Retrieved from https://www.blackrock.com/sg/en/introduction-to-blackrock

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). *Contingency planning guide for federal information systems* (No. NIST SP 800-34r1). https://doi.org/10.6028/NIST.SP.800-34r1

Wheatley, M. (2003). British Telecom’s Termination Checklist. Retrieved from CSO Online website: https://www.csoonline.com/article/2122571/british-telecom-s-termination-checklist.html

Whitman, M. E., & Mattord, H. J. (2018). Management of Information Security, 6th Edition [VitalSource Bookshelf version]. Retrieved from vbk://9781337671545