**BlackRock INC. Strategic Cybersecurity Plan**

**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](#_Toc44346266)

[Company Description 4](#_Toc44346267)

[Business Mission, Vision, and Values 5](#_Toc44346268)

[IT Philosophy 6](#_Toc44346269)

[Company Organizational Chart 8](#_Toc44346270)

[Security Organization Description 10](#_Toc44346271)

[Security Mission Statement 11](#_Toc44346272)

[Security Vision Statement 11](#_Toc44346273)

[Security Core Values 11](#_Toc44346274)

[Cybersecurity Team Organizational Chart 12](#_Toc44346275)

[Security Organization Justification 14](#_Toc44346276)

[Security Issues and Challenges 16](#_Toc44346277)

[References 19](#_Toc44346278)

# Introduction

BlackRock Incorporated is a global leader in the 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 integrated these tools with various product structures such as mutual funds and distinct institutional and individual investment accounts. Additionally, our industry-leading ETF platform: iShares, and various other pooled investment tools continue to deliver exceptional results that seemed impossible once.

As we continue to put our clients first, we also aim to be exceptional in achieving a well-established balance between opportunities and risks. We approach investments based on a strong belief that we can acquire key market insights as well as utilize our unique strategies to identify, detect, and respond to risks. As such, we continue to satisfy leadership risk management goals and meet critical performance in all market environments.

Furthermore, as a multinational institution, we efficiently utilize the advantages of continuously forming local relationships and global reach to deliver services that allow us to manage clients’ assets across seven main continents. This has allowed us to keep the independence BlackRock needs to maintain our commitment to focusing on clients with high performing investments. As such, we continue to operate without one single major stockholder, instead, many autonomous directors.

That said, we also understand our clients’ concerns about 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 maintain the privacy and security of such data by employing advanced technical controls, industry security standards, and a strong culture of pre-established policies and procedures aligned with BlackRock’s business elements.

On behalf of our Board of Directors and I, thank you again for your confidence in BlackRock.

Sincerely,

*Laurence D. Fink*

Chairman and Chief Executive Officer.

# Company Description

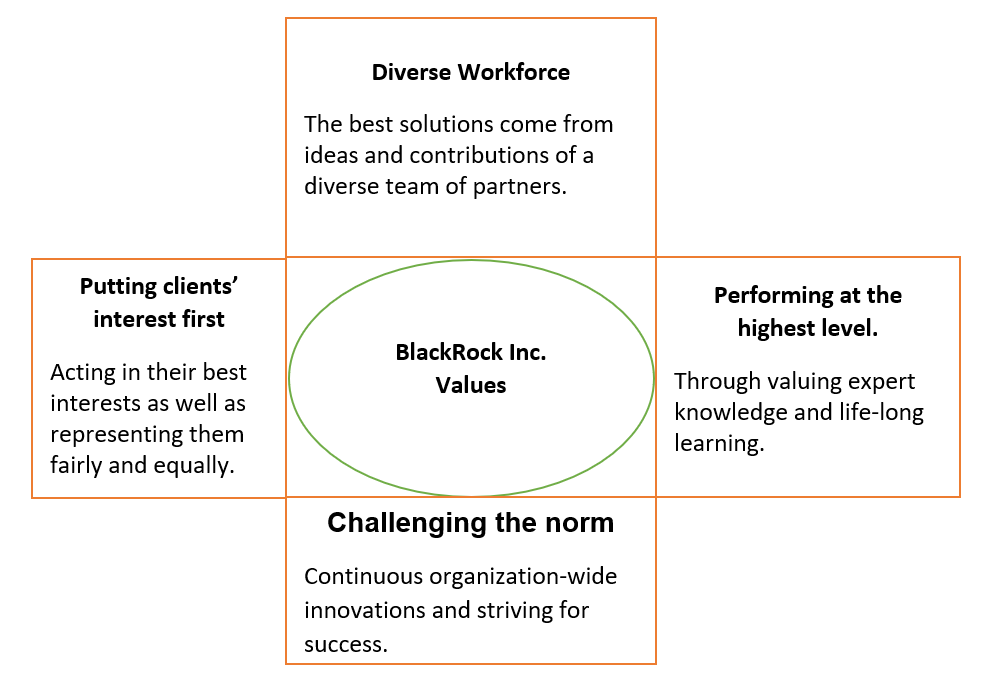
Founded in 1988 by Laurence D. Fink and seven other partners, BlackRock has expanded to be a trusted institution that manages more money than any other investment firm in the world. The investment management company is headquartered in New York, USA. It provides solutions ranging from essential and measurable active management methods that enhance performance to optimized indexing plans created to achieve comprehensive exposure to world capital markets (BlackRock Incorporated, 2019). The company currently has about 13,000 associates with offices in 30+ countries around the world (“Introduction to BlackRock”, n.d.).

# Business Mission, Vision, and Values

**Mission:** BlackRock’s mission is to create a better financial future for our clients (“Mission and Principles”, n.d.).

**Vision:** BlackRock’s purpose is to provide financial well-being to a growing number of people. We dedicate ourselves to protecting and growing the value of clients’ assets, thereby allowing them to form a trust in the work we do (“BlackRock Mission, Vision & Values”, n.d.).

**Values:** BlackRock’s values originate from the key elements depicted in the diagram below.



# IT Philosophy

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). In fact, for BlackRock, information technology continues to be at the forefront as the company leads in investment management by handling money that is more than the GDP of some countries.

To provide these exceptional solutions, BlackRock’s products and services depend on a hybrid cloud infrastructure with the company’s business operation running on an Aladdin Enterprise operating system. Additionally, part of this infrastructure is offered to clients and internal business units as Software-as-a-Service (SaaS). A summary of these technologies and the services they offer is shown in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| Technology | Deployment Environment | Provided By | Purpose |
| Aladdin Enterprise | Hybrid cloud infrastructure | Amazon Web Services (AWS) | Analyzes investment risks by considering the market conditions, news, and weather conditions.  Connects the information, people, and technology needed to manage investments in real-time. |
| SaaS solutions | Hybrid cloud infrastructure | Microsoft, Google, Amazon Web Services (AWS) - computing technologies such as Red Hat Enterprise Linux, the Akamai Content Delivery Network, and SAP solutions. | Provides micro-investment platforms that connect a wide range of investors, big and small. |

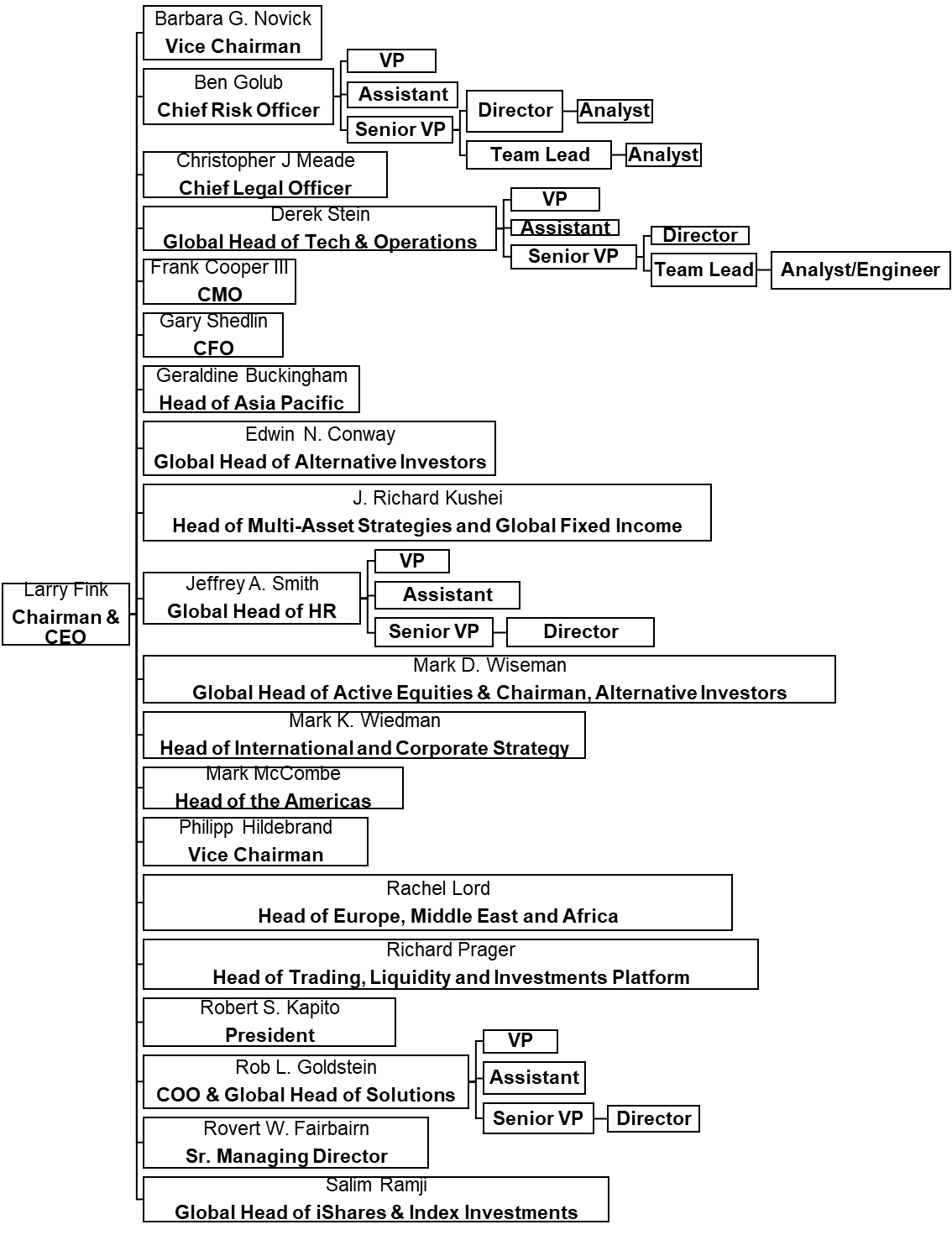
On the other hand, some technology functions, such as BlackRock’s SWIFT messaging network, used to manage assets from wealth funds and pensions, are outsourced and maintained by Computacenter PLC. In the same manner, the company’s platforms that manage sales data are planned to be outsourced to leading technology providers such as SAP software solutions.

Hence, BlackRock’s heavy reliance on the use of information technology products and services is critical to run the company’s day-to-day activities. Such activities include powering fast allocation of assets, risk management of assets, and interactive platforms. These products, services, and technologies are, in turn, used to fulfill BlackRock's mission and values.

# Company Organizational Chart

BlackRock is a large organization consisting of various members belonging to the Global Executive Committee and the Board of Directors (BlackRock Leadership, n.d.). As a result, the organizational chart shown below focuses on key positions held within the company.

The organizational structure is constructed beginning with the leadership team and board of Directors who are responsible for the various major business functions, operations, and units, followed by Senior Vice Presidents, Vice Presidents, and Assistants reporting to them. Additionally, below the Senior Vice Presidents and Vice Presidents, are Directors and Team Leads managing sections of business areas. These folks are then subsequently followed by analysts and engineers who are directly responsible for most of the daily monitoring and maintenance of BlackRock’s systems (“BlackRock - Org Chart”, n.d.). Additionally, while several teams have openings, the company continues to recruit skilled professionals who share the same visions as associates.



This reporting structure is effective as it empowers networks within BlackRock that are essential to achieve the critical outcomes of the company. The organization has sufficient resources to empower accountable leaders with their delivery teams providing results in such a way that BlackRock can continue to promote loyalty and better financial future for customers. Hence, the above organizational structure is the best for the company. It allows the need to reinforce the organization's strategic vision and priorities.

# Security Organization Description

The information security department at BlackRock plays a critical role in ensuring the company’s products and services are of the utmost importance for the organization's success. The department supports the company’s corporate philosophy and principles in its commitment to protecting BlackRock’s compute and network infrastructure from damaging activities, intended or otherwise by equipment or individuals, which could threaten its business operations and continuity.

Additionally, the department handles the responsibility of protecting corporate, clients’, and employees’ data that can reside in computer systems (both connected and not connected), including but not limited to computers (such as laptops, tablets, and desktops), hot-plug devices (such as USB drives, keyboards, mice, and external drives), network, email, and social media accounts, as well as any related activities that are the property of BlackRock Inc. As such, the information security team enforces that such systems get used only for purposes that serve the business operations and only during regular working hours.

Furthermore, to attain these objectives, the department also upholds the following security mission and vision statements as well as key core values that enhance and support BlackRock’s cybersecurity program.

## Security Mission Statement

The functions of the information security department are implemented with the ideology to Identify, assess, and proactively manage the risks to BlackRock's information systems and information, enabling the company to succeed in its mission of creating a better financial future for clients.

## Security Vision Statement

The purpose of the information security department is to securely store and protect the value of clients’ assets and business data, thereby earning their trust as the company continues to provide financial well-being to a growing number of people.

## Security Core Values

To achieve the cybersecurity unit's mission, the following values are at the core of the department’s operations.

1. **Exceptional Service:** Clients come first at BlackRock; likewise, the various business units supported by the team are primary to ensure business operational excellence for the entire organization.
2. **Openness and Growth:** Life-long learning is a value adopted by the whole organization. The same value applies to the cybersecurity unit with the addition of encouraged sharing of information and intelligence between the various security functions. This will ensure a quick response and a more proactive posture to the ever-changing threats faced in the company’s infrastructure.
3. **Robust Systems:** The information technology systems at BlackRock are designed to be flexible to changes in state and location, as well as resilient within their operating environment. To achieve this, testing is an essential operation of the cybersecurity unit, aiming to validate and ensure that the technology systems at BlackRock can withstand different stresses and attacks.
4. **Excellence in Systems’ Operations:** Given the time-sensitive nature of investment management, BlackRock’s computer systems' reliability is of high importance. As a result, the operations undertaken within the information security unit are to be accomplished while ensuring the highest availability of the technologies. This means prioritizing the availability of services and employing the confidentiality and integrity of information systems while meeting acceptable security standards.

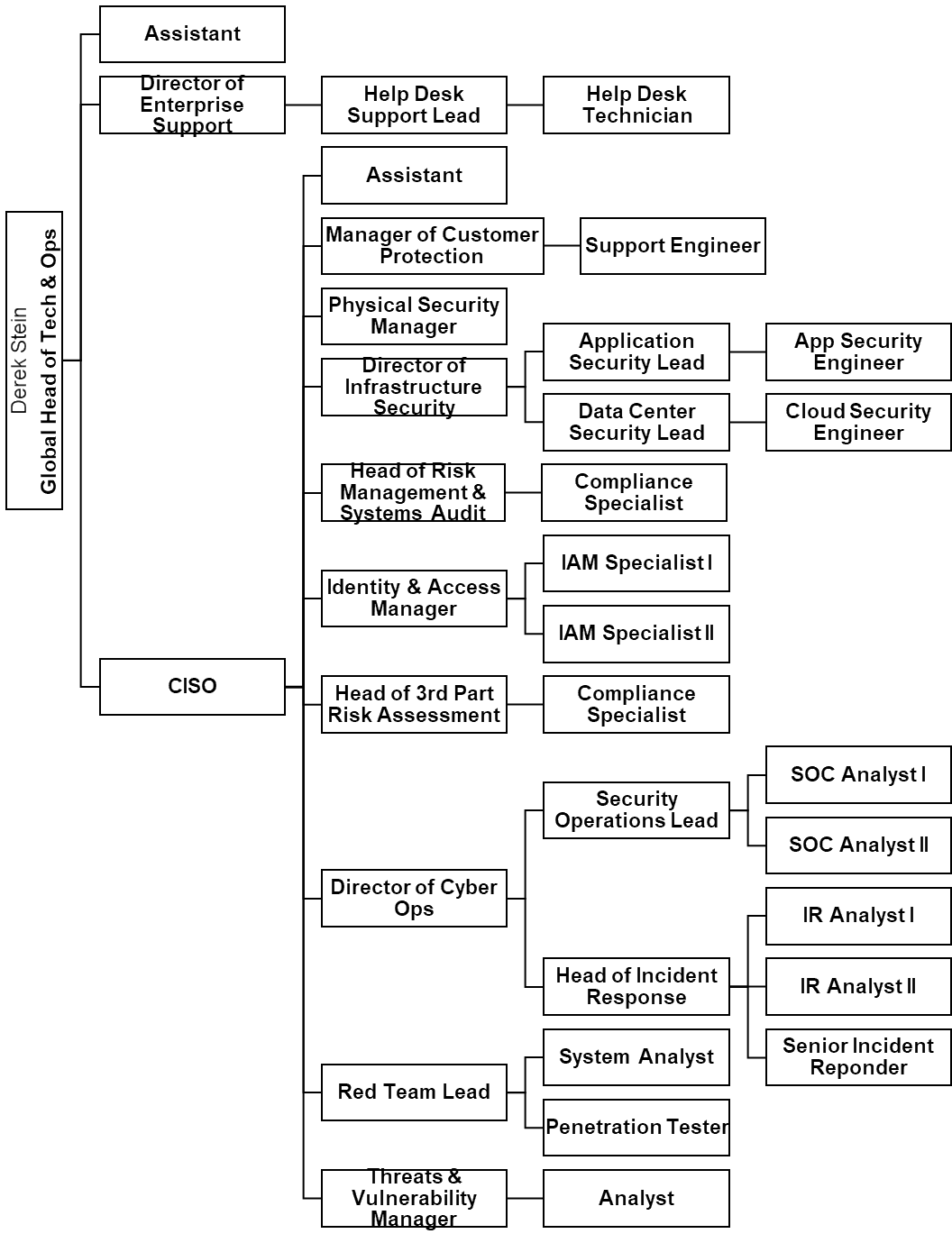
## Cybersecurity Team Organizational Chart

The cybersecurity department's functions are separated between the internal technology unit, which consists of the Chief Operating Officer and Global Head of Solutions (as shown in the BlackRock’s organizational chart above), and the external technology unit, which contains the Global Head of Technology and Operations.

The internal technology unit is responsible for enterprise security. It entails the enterprise information security functions such as application security engineering, systems audit, and help desk support. Some of these roles can also operate under the global head of solutions depending on the daily business operations.

On the other hand, the external technology unit is responsible for global information security team functions reporting to the Global Head of Technology and Operations. The team is responsible for carrying out crucial tasks such as identity and access management, conducting third-party risk assessments, and ensuring compliance with international standards and laws. This team also houses cyber operations such as vulnerability management, incident response, and threat management. Additionally, while some of these teams have openings, the department continues to work with human resources to recruit skilled security professionals who share BlackRock’s visions.

That said, the number of all the security staff involved can be extended to 500+ associates given the global scale, size, and complexity of the information technology involved. As shown below, the reporting structure fits the information security staffing needs of a large organization, such as BlackRock, by effectively enforcing separation of duties and guiding the department to make security decisions based on plans and policies integrated with the organizational culture (Whitman & Mattord, 2018).



Furthermore, the cybersecurity team has sufficient resources dedicated to maintaining the large number of staff, which continue to support BlackRock’s aim of loyalty and better financial future for customers. Hence, the above organizational structure is the best for the team as it upholds the needs to reinforce the strategic vision and priorities of the organization.

# Security Organization Justification

Due to the large number of business operations conducted by BlackRock and the various IT systems used to support such activities, the organization's security function has been separated into two different groups.

The first of these groups is the internal technology unit, which is responsible for enterprise security and entails the enterprise information security functions. As shown in the cybersecurity team organizational chart above, this group hosts security roles such as application security engineering, systems audit, and help desk support. Some of these roles can also operate under the global head of solutions depending on the daily business operations. Hence, these professionals ensure the secure function of software application programs and systems, evaluate, improve their effectiveness, and ensure compliance in the environments that BlackRock operates in to avoid legal penalties. The group also provides 24/7 support for clients and employees who encounter technical issues in their day-to-day interactions with corporate resources.

The second of these groups is the global information security unit. This group is responsible for managing the information security of the global IT assets and any externally facing technologies that the organization uses to conduct its businesses. As shown in the cybersecurity team organizational chart above, this group hosts security roles such as Incident Response (IR) and Security Operations Center (SOC) Analysts at different levels of support due to the vast amount of IT assets being managed, which requires different triage levels and various professional in charge at each level.

Additionally, due to the organization's IT philosophy being primarily hybrid cloud-based, another team dedicated to infrastructure security exists. The hybrid cloud infrastructure refers to mixed computing, storage, and services environment made up of BlackRock’s on-premises infrastructure (data centers), and a public cloud (Amazon Web Services (AWS)). Furthermore, a physical security manager role was established due to BlackRock having its own data centers in multiple area zones to house a powerful investment management operating system and platforms used by clients worldwide, requiring rigorous physical security to maintain compliance. Finally, under the Global Head of Tech and Operations with the Chief Information Security Officer (CISO) as lead, other security roles such as risk assessment, red team threat management, and vulnerability management functions exist to oversee testing of the applications and products developed by BlackRock such as Aladdin OS and iShare ETFs (“Introduction to BlackRock”, n.d.).

Hence, it remains the CISO’s responsibility to see that the information security functions are adequately performed within the organization. However, not all security functions will be hosted under the CISO. An example of this is the help desk technician, who provides support for clients and employees who encounter technical issues and need to have their passwords reset. This responsibility will fall under the Chief Information Officer (CIO) working with the enterprise support staff, which is led by a director of enterprise support, who also works very closely with the information security unit. As a result, responsibilities can sometimes be tied together according to a standard banner that describes the aim of the information security department.

# Security Issues and Challenges

Due to its size and global business activities, BlackRock faces potential threats from fluctuating investment and world economy, as well as changing rules and reforms. The company also faces risks arising from technologies, third-party interactions, and security breaches (BlackRock Inc SWOT Analysis, 2019). Hence, BlackRock has always remained cognizant of the potential security issues and challenges headed toward its way. That said, however, the following issues and challenges are in-scope presently, and the company has been mitigating and responding to them through several means of controls such as physical (secure data centers), administrative (policies and procedures), deterrent (cameras and security guards), preventive (network security tools), detective (logs and audit trails), and recovery (backup systems and data) (Dempsey, Nieles & Pillitteri, 2017).

1. Cyber Attacks: One of the threats that BlackRock faces is a cyber-attack on its telecommunication and computer systems. Such attacks can result in the disruption of business operations and potentially cause financial losses, as well as disclose or alter intellectual, confidential, or competitive data. These attacks can be caused by malware, denial-of-service attacks, phishing, ransomware, or even by employees unintentionally. They can adversely impact BlackRock’s bottom line with losses resulting from legal penalties (Butler, 2017).
2. System Upgrade Complications: Another threat that the organization faces comes from the upgrade process of crucial computer systems. Due to BlackRock’s reliance on select key technologies such as Aladdin OS and the iShares trading platform, the system upgrades and protection measures in place can potentially cause disruption and introduce security issues. Such issues could result in downtime of critical operations as well as affect clients’ trust in BlackRock.
3. Third-party Challenges: Unavailability or failure of technical dependencies from third parties is another security challenge that BlackRock faces. This can harmfully affect BlackRock's essential product: Aladdin OS. It could lead to the loss of clients, hinder growth, and productivity, as well as affect brand image. Aladdin depends on inputs from various third parties for analysis and predictions. As such, the disruption of related information flows could result in difficulty in operations carried out by Aladdin. It can also hamper BlackRock's ability to provide investment advisory services to internal and external clients.
4. Technology Advancements: With the continued enhancement to Aladdin's abilities and its expansion into new markets and locations, its processing scale has grown significantly. It may expose BlackRock to greater regulatory scrutiny and increased risk concerning managed data, information security, and business operations. If left unaddressed, the company will be unable to maintain the platform's stability and operational resilience. This scenario may result in loss of clients, reduced business legal fines or sanctions, and tarnish BlackRock's brand image, directly affecting earnings and revenue.

# References

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

BlackRock Inc SWOT Analysis. (2019). *BlackRock, Inc. SWOTS Analysis*, 1–7. Retrieved from http://search.ebscohost.com.dbproxy.udallas.edu/login.aspx?direct=true&db=bth&AN=136370419&site=ehost-live&scope=site

BlackRock Leadership. (n.d.). Retrieved from https://www.blackrock.com/corporate/about-us/leadership

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

BlackRock - Org Chart. (n.d.). Retrieved from https://theorg.com/org/blackrock

Butler, M. (2017). Ransomware Attacks Put NY Cybersecurity Regs in Spotlight. Retrieved from https://www.intelligize.com/ransomware-attacks-put-new-york-cybersecurity-regs-spotlight/

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/

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

Mission and Principles. (n.d.). Retrieved from https://www.blackrock.com/institutions/en-axj/mission-and-principles

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