**BlackRock INC. Risk Assessment**

**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](#_Toc45557717)

[Identification of Assets 3](#_Toc45557718)

[Classification of Assets 5](#_Toc45557719)

[Vulnerability of Assets 7](#_Toc45557720)

[Mapping Vulnerability, Probability of Occurrence, and Impact to Assets 9](#_Toc45557721)

[Risk Mitigation Strategy 11](#_Toc45557722)

[Risk Mitigation Recommendations 14](#_Toc45557723)

[Summary 16](#_Toc45557724)

[References 17](#_Toc45557725)

# Introduction

In the process of conducting various business operations, BlackRock faces information security risks, which could endanger the integrity of data at hand or threaten the company’s very existence. As a response to such events, this document details the security vulnerabilities in assets and the risks they pose as it applies to the company. It also presents mitigation strategies that can be used to overcome them.

In discussing risk, however, it is first essential to understand what it entails. According to ISACA’s *COBIT 5 for risk* (2013) publication, risk is “the probability of an event and its consequence”, with such events resulting from the adoption, ownership, involvement, impact, and usage of information technology (IT) in the business activities of an organization (*COBIT 5 for risk*, 2013). As a result of such circumstances, risk is an inevitable byproduct of using IT to conduct business. For BlackRock, this scenario is inherent, given that most operations involve technology.

# Identification of Assets

As the world’s leading financial services and investment firm, BlackRock faces various risks from the information assets it employs in conducting business activities. In this context, an asset is anything that has value to the owner of it. For BlackRock, the following are some of the assets that the company employs. They are outlined in relation to related components and specific examples as follows:

|  |  |  |
| --- | --- | --- |
| **Asset** | **Components** | **Examples** |
| Sites | * Web Servers * Domain Name | * External Internet Website |
| Databases | * Configuration Files * Operating System Resources * Software Keys | * Customer Database * Human Resources Database * Sales Database * Development and Production Databases |
| Networks | * Networking Interfaces (Ports and Jacks) * Network Devices (Routers, Firewalls, Switches, and Access Points) * Network Links | * Local Area Network * Wide Area Network * Virtualized networks (Cloud-based – VMware NSX) * Intranet |
| Applications | * Source Code * Software Keys * Operating System Resources * Configuration Files | * Internal Applications * Desktop Applications * Web Applications * Operating Systems (Aladdin OS) |
| People | Employees and Non-Employees | * Trusted Employees * Contractors * Vendors * Guests |

Among the above-described group of assets (with related components and examples), the following are key to BlackRock’s success.

1. **External Internet Website:** Through various linked pages, Blackrock’s public website is designed to offer various services from company information to market insights, investment strategies, and resources and tools clients can utilize for financial services. More importantly, the site contains a portal that clients can log-in to their respective accounts to manage their communications, funds, and investment options. Hence the site contains sensitive financial information of clients in compliance with the Gramm-Leach Bliley Act (GLBA).

Additionally, the site is hosted by BlackRock’s web servers that house the database containing customer data and files that provide services to the clients of BlackRock. Hence, this asset is vital due to the critical role it plays in providing a gateway for the clients to access their subscribed services. It can have a big impact on finances if these critical services are down since they are used to advance clients’ businesses in alignment with the company’s unique guidelines.

1. **Virtualized Networks:** This category of assets includes the local cloud-based networking hosted within BlackRock and is used to provision private cloud instance connectivity across business units, clients, and developers. This is important since virtual networks serve as the link between IT systems for conducting operations. Without their proper functioning, business activities would be hindered, and internal units would be unable to carry out their job duties.
2. **Aladdin Operating System (OS):** This operating system software 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. This asset is valuable because it brings in a significant amount of revenue for the company: approximately $785 million (BlackRock Incorporated, 2019).
3. **Human Resources (HR) Database:** This database hosts an organized collection of data pertaining to both internal and external personnel. This asset is important due to the various legal standards, federal, and local laws that BlackRock is subject to, given the nature and geographical location of its business operations. Examples of such laws and standards include the Gramm-Leach Bliley Act (GLBA) and the General Data Protection Regulation (GDPR), which stipulate that investors' identifiable information should remain confidential with the consequence of legal fines if the data is leaked.
4. **Trusted Individuals:** This category includes corporate employees, asset managers, investors, and other stakeholders of the company involved in making decisions. Due to the sensitive level of access that these employees are given to carry out their duties (such as the source code for Aladdin OS and insider information on trades), they are an essential asset whose risk needs to be assessed and managed.

# Classification of Assets

The information assets identified above are classified according to the sensitivity of the data they store or manage, along with their impact on the profitability of the company. The security techniques and sensitivity of the data is based on the categorization of related information asset according to the following scheme:

* Public – This is information that is unclassified and meant to be consumed by the public. It has no damage to the company’s operations, mission, or existence.
* Internal – This is information intended to remain and be used only internally within the company. This type of information can cause serious but not existential damage to the company.
* Sensitive – This is information that is neither public nor unclassified. Its leakage can cause some damage to the company but not as much as the higher-level classifications.
* Confidential – This is information that is most sensitive and is to be used or accessed based on clearance level. This type of information can cause serious damage to the company if leaked.

The above data classification scheme is combined with the criticality of the assets based on the profitability and business impact they introduce to the organization. These categories are described as follows:

* Low – This is an asset that either does not generate revenue or generates very little of it and is not expensive to replace. Additionally, its liability causes little or no damage to the BlackRock’s bottom line.
* Medium – This is an asset that generates moderate revenue and is relatively expensive to replace or has a liability that moderately damages the company's bottom line.
* High – This is an asset that generates significant revenue and is costly to replace or has a liability that significantly impairs the company's bottom line.
* Critical – This is an asset that generates the most revenue and is also the most expensive to replace. It also has a liability that can immensely damage the bottom line of the company.

In summary, the above assets are classified and categorized, as depicted in the matrix below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Low** | **Medium** | **High** | **Critical** |
| **Public** | - | - | - | - |
| **Internal** | - | Virtualized Networks | - | - |
| **Sensitive** | - | - | External Internet Website | - |
| **Confidential** | - | HR Database | - | Aladdin OS  Trusted Individuals |

Impact

Data

Classification

As shown in the table above, the virtualized networks are classified as internal due to the data passing through it being private to the company. Additionally, while it can somehow hinder operations that generate revenue, its impact on profitability is low, and it is relatively expensive to replace.

On the other hand, the external sites are classified as sensitive as they contain some information that is not meant to be public and unclassified. However, they also contain access credentials and customer information that can have a high negative impact on businesses and trust in BlackRock. Additionally, In the event of a leak, the impact on profitability can damage the company, such as its brand image. However, the damage is not as serious as an existential threat.

As for the HR Database, the classification is confidential once again due to the sensitive information stored, such as social security numbers and addresses. The impact on profitability is medium, as it does not generate revenue. However, the liability of the data being leaked moderately damages the company and can result in potential lawsuits.

Finally, Aladdin OS is classified confidential due to the sensitive information used in transactions such as credit card numbers and social security numbers for enrollment. Additionally, according to BlackRock’s 10-k report of 2018, the system provides a significant profit source. Differently, trusted individuals are also within the confidential-critical category due to their significant knowledge about the company, its systems, and business processes, which can result in a serious amount of fatal damage to BlackRock.

# Vulnerability of Assets

The above-categorized assets pose a risk to BlackRock because of the vulnerabilities they continuously face. That is, multiple vulnerabilities exist for each asset. However, for the purpose of this document, the most critical vulnerabilities will be discussed as follows:

1. **External Internet Website:** When it comes to the company’s public site, the most critical vulnerabilities are:
   * Remote Code Execution (RCE): The web servers that host such sites are vulnerable to RCE, the capability of executing code on the operating system, remotely without proper permissions, and bypassing authorization. This vulnerability may be present due to the multitude of libraries and components that make-up the applications needed to serve web requests such as Apache, Nginx, and Laravel or Flask. Hence, this vulnerability is critical. It can allow an attacker to take down the web servers themselves or exfiltrate the sensitive information they contain.
   * Broken Authentication: This vulnerability includes weak authentication processes and poor session management that can allow attackers to compromise credentials or impersonate users. Such vulnerability can allow an attacker to escalate privileges and gain access to clients’’ sensitive financial data as corporate information (Gross, 2019).
   * Unauthorized Forwards and Redirects: If the web servers fail to validate requests to redirect and forward users to BlackRock’s sites, attackers can make use of this weakness to redirect clients to phishing or malware sites to steal their information. Such events can significantly damage the reputation of the company in the services it provides. Additionally, it can introduce legal consequences to BlackRock due to the leakage of sensitive information.
   * Components with Unknown Vulnerabilities: Modules such as APIs (Application Program Interfaces) who exhibit unknown vulnerabilities can lead to zero-day exploits. This is a serious vulnerability as there might not be security patches available to apply, leading to corporate and client data loss or web servers’ takeover by intruders.
   * Product Weaknesses: BlackRock utilizes various vendor products to uphold the integrity and security of systems. However, if such tools fail to provide sufficient logs, it can result in suspicious web activities going unnoticed. This is an extremely serious weakness that does not come to attention unless the company experiences an incident and is unable to diagnose it. Suspicious activity endangers end users, data, and the systems it resides on. As a result, BlackRock needs to continue to pay attention to such vulnerabilities.
2. **Virtualized Networks:** The biggest vulnerability in virtualized networks is a misconfiguration. It is the incorrect configuration of computer service or asset with no security hardening implemented or unnecessary, and default features left enabled.

This vulnerability is dangerous because it is easy to overlook and very common in virtualized environments. Often, the software used in virtualization comes out of the box with default user credentials, and various security hardening controls disabled for reasons such as compatibility, set-up, and ease of use.

1. **Aladdin Operating System (OS):** The home-grown operating system’s most concerning vulnerability is also RCE. This vulnerability is a significant concern as industry-leading, and confidential clients rely on the operating system to securely manage their investments, given the sensitivity of the information they provide. Additionally, BlackRock itself relies on it to make investment decisions and market moves, making it essential to protect against such vulnerability exploitations.
2. **Human Resources (HR) Database:** The HR Database’s most concerning vulnerability is SQL Injection. This is an injection attack using SQL statements to modify or retrieve information from a database without proper permission.

The Structured Query Language (SQL) is the primary method of accessing, modifying, adding, and retrieving data from the database. As such, this needs to be secured to ensure that the personally identifiable information held within the database is secure. SQL injection is the most worrisome as it is the topmost common vulnerability exploited in databases in the wild, according to OWASP top 10. Additionally, this vulnerability can insert malicious content that can infect end users (OWASP, 2017).

1. **Trusted Individuals:** The most significant vulnerability related to trusted individuals is phishing. This is the fraudulent attempt to get sensitive data by disguising as a trustworthy individual or entity. This vulnerability is worrisome because people are usually susceptible to well-crafted messages designed to request or still information directly. Hence, given that such individuals, such as employees, are entrusted with privileged access to classified information, unauthorized access to their credentials or information via phishing is a great concern as it can easily damage BlackRock.

# Mapping Vulnerability, Probability of Occurrence, and Impact to Assets

Mapping out the vulnerabilities of the assets described above in terms of the probability of occurrence and the potential impact it can have is a key strategy to uphold BlackRock’s security objectives and support its business operations. This technique is presented with a table mapping out all assets against the probability of occurrence and potential impact variables described below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Likelihood Score** | **Label** | **Probability** | **Description** |
| 0 | Not Applicable | 0% in the upcoming 12 months | Never |
| 1 | Scarce | 5% in the upcoming 12 months | At least once every 20 years |
| 2 | Not Likely | 25% in the upcoming 12 months | At least once every 10 years |
| 3 | Moderate | 50% in the upcoming 12 months | At least once every 5 years |
| 4 | Probable | 75% in the upcoming 12 months | At least once every 2 years |
| 5 | Nearly certain | 100% in the upcoming 12 months | May occur several times in a year |

Additionally, the impact of the above vulnerabilities in the instance that they get exploited is described as follows.

|  |  |  |
| --- | --- | --- |
| **Impact Score** | **Label** | **Description** |
| 0 | Not Applicable | No impact |
| 1 | Inconsequential | No disclosure of sensitive data and no interruptions |
| 2 | Minor | Multi-minute disruption and no disclosure of sensitive data |
| 3 | Moderate | Multi-hour disruption and some disclosure of sensitive data |
| 4 | Extensive | Single day disruption and disclosure of sensitive data |
| 5 | Fatal | Multi-day disruption and serious disclosure of sensitive data |

Based on the above two tables, the vulnerabilities described for each asset can be summarized as follows.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset** | **Data Classification** | **Vulnerability** | **Likelihood** | **Impact** |
| External Sites | Sensitive | RCE  Broken Authentication  Unauthorized Forwards and Redirects  Unknown Vulnerabilities  Product Weaknesses | Probable  Scarce  Scarce  Nearly Certain  Nearly certain | Moderate  Minor  Minor  Moderate  Extensive |
| Virtualized Network | Internal | Misconfiguration | Nearly certain | Moderate |
| Aladdin OS | Confidential | RCE | Moderate | Fatal |
| HR Database | Confidential | SQL Injection | Probable | Extensive |
| Trusted Individuals | Confidential | Phishing | Nearly certain | Fatal |

The reason behind the categorization of these vulnerabilities in terms of likelihood and impact is detailed below.

**External Internet Website – [RCE, Broken Authentication, Unauthorized Forwards and Redirects, Unknown Vulnerabilities, Product Weakness]**

Remote Code Execution (RCE) is likely to happen at least once every two years because of the multiple libraries and files involved in web applications and web hosting. The impact in this situation is moderate, as only a few hours of downtime/disruption is expected along with some sensitive data disclosure.

On the other hand, unknown vulnerabilities or zero-day exploits and weakness in products are almost certain to occur with vendors providing patches and upgrades to overcome such weaknesses. While unknown vulnerabilities can be mitigated from exploitation by other controls in place resulting in moderate impact, vulnerabilities in monitoring and logging of security tools can have an extensive impact until the cause of the incident is identified.

Finally, when it comes to broken authentication and unauthorized forwards and redirection of web pages, they are highly unlikely (scarce) to occur due to BlackRock’s deployed network security solutions. Hence, their impact is minor, resulting in minimal disruption and no disclosure of sensitive data.

**Virtualized Network – [Misconfiguration]**

Misconfiguration is very common and likely to happen due to the nature of people being prone to errors. That is, system practitioners in charge of tool set-up are prone to making mistakes during the configuration of the virtual network devices. However, the impact is not severe, and it usually takes a couple of hours for someone to correctly configure the tool, test it, and verify that it is fixed.

**Aladdin OS – [RCE]**

Remote Code Execution (RCE) is possible once every five years given the multitude of dependencies entailed in the operating system. A quick look up in the CVE website reseals that this issue has happened within a difference of 5 years (“Aladdin Enterprises: Security vulnerabilities”, n.d.). That said, the impact is rated as fatal because it takes several days to get all dependencies checked, fixed, and verified.

**HR Database – [SQL Injection]**

An SQL injection is the topmost common vulnerability exploited in databases in the wild, according to OWASP top 10. It is also likely to happen once every two years. That said, with the large-scale software development that takes place in the company, there is a high chance of some code will be vulnerable to unexpected SQL injection. The impact of such vulnerability is extensive due to the definite day or two that it will take to fix and verify that the confidential data is secure.

**Trusted Employees – [Phishing]**

Phishing is very likely to happen due to the imperfection of people. That is, the multiple phishing attacks expected on BlackRock means that it is almost certain to occur in terms of likelihood. Hence, given the very high level of sensitivity that users have based on their role, the ranking for phishing becomes fatal, disclosing serious, sensitive data.

# Risk Mitigation Strategy

Given that BlackRock continuously faces a certain level of risk due to its extensive depends on assets such as IT systems and stakeholders, the company employs the risk mitigation approach shown below to combat the vulnerabilities posed by assets.

|  |  |  |
| --- | --- | --- |
| **Mitigation Score** | **Label** | **Description** |
| 0 | Not Applicable | The risk does not apply to the organization’s assets |
| 1 | Transferable | The risk can be handled by the organization’s cyber insurance |
| 2 | Avoidable | The risk must be avoided as it presents unwanted negative consequences to the organization. |
| 3 | Acceptable | The risk can be accepted as necessary though potentially unpleasant to the organization |
| 4 | Reducible/ Controllable | The risk must be mitigated through security solutions, policies, and processes due to the severe consequences it brings |

On the other hand, the uncertainty score (calculated between 0 -100 percent) indicates the accuracy of the assumptions and data collected regarding the vulnerability. Hence, as depicted in the chart below, an uncertainty score of 0% indicates that the assumptions and data collected regarding the vulnerability are 100% accurate. On the other hand, an uncertainty score of 100% means that the assumptions and data regarding the identified vulnerability are entirely inaccurate. These data points are extremes, and most often, we expect the uncertainty score exclusively between 0 and 100 percent.

Hence, BlackRock’s asset vulnerabilities can be summarized as follows regarding mitigation and uncertainty approaches.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset** | **Vulnerability** | **Risk Mitigation Score (0-5)** | **Estimated uncertainty Score** | **Description** |
| External Sites | RCE  Broken Authentication  Unauthorized Forwards and Redirects  Unknown Vulnerabilities  Product Weaknesses | 4  3  3  3  3 | 20%  90%  90%  10%  10% | RCE poses a serious risk that must be controlled to avoid fatal impacts. It also has about a 75% occurrence in the coming 12 months.  Broken authentication can lead to unwanted exposure of session information to unauthorized users. While the risk is scarce to occur due to strong technical controls, it is still acceptable and can be mitigated easily.  Unauthorized forwards and redirects can trick users into accessing malicious sites. Although this risk is also scarce to occur due to strong technical controls, it is still acceptable and can be mitigated easily by investigating web traffic.  The components that make up the service tools are nearly certain to have an unknown weakness that can potentially favor attackers. However, there is no means for any organization to avoid them entirely. As a result, this risk is accepted, and appropriate mitigation strategies are applied as soon as they are available.  Vendor products are nearly certain to have weaknesses that can potentially be exploited by attackers. Such risks are accepted, and temporary mitigation strategies may be applied until the vendor provides patches and upgrades to overcome their products' weaknesses. |
| Virtualized Network | Misconfiguration | 4 | 30% | Misconfiguration is common, almost certain to occur, and poses a serious risk that must be controlled to avoid fatal impacts. |
| Aladdin OS | RCE | 4 | 70% | RCE poses a serious risk that must be controlled to avoid fatal impacts. According to the data collected regarding the vulnerability, it also has a high occurrence rate of once every five years given the multitude of dependencies entailed in the operating system. |
| HR Database | SQL Injection | 4 | 50% | Due to the large-scale software development that takes place at BlackRock, there is a high chance of some code will be vulnerable to unexpected SQL injection. It is likely to happen once every two years (OWASP, 2017). Such an event can have extensive risk in leaking confidential data and must be controlled or reduced using appropriate mitigation strategies, including the utilization of smart security solutions. |
| Trusted Individuals | Phishing | 4 | 10% | According to BlackRock’s collected data, phishing is also certain to occur to trick users into providing sensitive information. It introduces a significant risk that must continuously be reduced and controlled via security awareness, policies, and technical solutions to avoid fatal impacts on the organization. |

In conclusion, by incorporating the mitigation score and uncertainty score with the likelihood and impact score for each asset’s vulnerability, a risk score (0 to100) can be computed, as shown in the table below.



# Risk Mitigation Recommendations

In response to the above-identified risks, the following risk mitigation strategies and controls are recommended.

|  |  |  |  |
| --- | --- | --- | --- |
| **Asset** | **Vulnerability** | **Mitigation Controls** | **Description** |
| External Sites | RCE  Broken Authentication  Unauthorized Forwards/Redirects  Unknown Vulnerabilities  Product Weaknesses | Web application firewall (WAF)  Regular penetration testing  Regular penetration testing  Strong password policy  Disallow Offsite Redirects  Preventive security practices  Disaster recovery procedures  Evaluate vendor risks  Frequent back-ups | Here, a web application firewall is an added layer of security with filtering rules that drop malicious requests.  On the other hand, regular penetration testing entails regularly looking for the weaknesses in the web servers and trying to exploit them with the intention of fixing them.  These controls are effective as they will first prevent the weakness from being taken advantage of through the WAF, and secondly, proactively look for any missed application vulnerabilities that often lead to RCEs.  Regular penetration testing, as described above, is critical to identify web application and session vulnerabilities.  Additionally, having a good password policy in effect is also essential, since it allows for defining an adequate level of password complexity and the implementation of a regular password rotation. This would help with brute force attacks and may also prevent the use of stolen credentials.  BlackRock should prevent to other domains by checking the URL being passed to the web servers redirect function. Additionally, Redirects to URLs passed in query parameters should only be triggered by pages on your site. Any other sites triggering a redirect should be treated with extreme suspicion.  These practices include keeping firewalls and antivirus protection up-to-date and matched carefully to corporate needs. Additionally, blocking attachments and managing external devices are also important. Furthermore, installing patches for on-premise systems immediately upon the issue and conducting vulnerability scans are also critical.  Furthermore, developing and practicing incident response that includes established roles and procedures is critical to mitigating the damage while it is happening.  It is crucial to evaluate vendor risks after initial onboarding continuously. A method must be chosen to evaluate vendors based on the risk category associated with each of them. This approach helps ensure that appropriate time, effort, and costs are allocated to each vendor risk category.  Additionally, while data security is paramount, data availability is also essential, especially because the damage that can be caused is uncertain and that clients need to access their data. |
| Virtualized Network | Misconfiguration | Change Management  Peer Review  Configuration Backup | A change management entails establishing procedures for changing configurations.  On the other hand, peer review entails having a peer examine the details of a configuration before putting it into production.  Additionally, backing up of configurations entails saving a copy of working and good configurations implemented for future reference or for reverting to previous configurations in the case of data loss.  These controls are effective as they will overcome the mistakes made by engineers implementing configurations, before going into production, and establish backups to use in the case of an incident. |
| Aladdin OS | RCE | Code Review  Regular penetration testing | Here, a code review refers to the examination of code developed for Aladdin OS.  On the other hand, regular penetration testing entails regularly looking for the weaknesses in Aladdin OS and trying to exploit them with the intention of fixing them.  These controls are effective as they will overcome the mistakes made by programmers before and after going into production, which is typically the root cause of RCE. |
| HR Database | SQL Injection | Code Review  Server-side input validation  Using APIs over database connectivity drivers | Here, a code review is the examination of code developed to access the database.  Server-side input validation is an additional code that checks received SQL statements to be processed for irregularities and either returns an error or drop them.  Additionally, an API avoids the database driver interpreter completely, via the use of an API to make requests which circumvent the flaw of SQL injection.  These controls are effective because they will either overcome the mistakes made by programmers through the code review or treat the malicious input, thereby preventing the vulnerability. |
| Trusted Individuals | Phishing | Intensified user awareness training  Deploy anti-phishing solutions  Multi-factor authentication | Here, more rigorous awareness training can be conducted, such as on a more frequent basis or using more advanced techniques to teach personnel to recognize and prevent phishing.  Additionally, anti-phishing solutions such as anti-spam filters, and safe browsing browser add-ons along with adware blockers, which can be used on the personnel’s devices and e-mail accounts.  Furthermore, multi-factor authentication involves trusted individuals using more than one factor when authenticating to various services.  These controls are effective as they decrease the attack surface with a more security-aware team and delay successful attacks by needing another authentication factor and filtering of phishing attempts. |

# Summary

BlackRock continuously faces risks arising from the use of various assets to conduct its daily business operations. Some of these key assets include external sites, virtualized network, the company’s Aladdin operating system, the company’s HR Database, and trusted individuals. These assets were first identified and analyzed from the perspective of data involved and the impact they have on profitability.

Second, the assets were assessed against the critical vulnerabilities they exhibit, the likelihood of such vulnerabilities being exploited, and the impact these weaknesses have on business activities. Following that, each asset’s current level of vulnerability based on existing controls and the estimated level of uncertainty based on the data collected regarding each vulnerability was carefully examined.

Additionally, each asset's risk score was calculated by incorporating the mitigation score and uncertainty score with the likelihood and impact score of their respective vulnerabilities. This analysis categorized risks as low, moderate, high, and critical, with phishing taking the critical level.

Finally, in response to the above identified risks, detailed risk mitigation strategies and controls were recommended for the organization to consider.

# References

Aladdin Enterprises: Security vulnerabilities. (n.d.). Retrieved from https://www.cvedetails.com/vulnerability-list/vendor\_id-32/Aladdin-Enterprises.html

BlackRock Incorporated. (2019). *Form 10-K 2018*. Retrieved from http://ir.blackrock.com/sec-filings

COBIT 5 for risk. (2013). Rolling Meadows, IL.: ISACA.

Gross, G. (2019). The 10 Most Commonly Exploited Web Application Vulnerabilities. Retrieved from https://blog.rapid7.com/2019/12/13/the-most-commonly-exploited-web-application-vulnerabilities-in-a-production-environment/

Kostadinov, D. (2016). Information and Asset Classification. Retrieved from Infosec Resources website: https://resources.infosecinstitute.com/information-and-asset-classification

OWASP. (2017). Top 10-2017 Top 10 - OWASP. Retrieved from https://www.owasp.org/index.php/Top\_10-2017\_Top\_10

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