Information Security Risk Assessment for PREDICTX Company

Student’s Name

Institutional Affiliation

Information Security Risk Assessment for PREDICTX Company

**Introduction the Case**

Information and system security are paramount in identifying, assessing, and implementing critical security controls in the applications. Understandably, security risk assessment help organizations to prevent application vulnerabilities and security threats. Therefore, performing a security assessment is an integral part of an organization's risk management processes. Identifying the risk associated with the information and computer systems is vital to identify information assets by understanding systems environment and systems interconnection/ information sharing (Wangen, 2017). Secondly, it is essential to perform system security level by identifying potential dangers, threats, or risks associated with the information and systems. Other aspects of systems security assessment include identifying existing security controls to mitigate the risk of threats in the exploitations of vulnerabilities. This paper aims to discuss information and systems security aspects of PREDICTX company, which is a micro-finance company. This paper also aims to provide a comprehensive report on information security risk assessment for the company under consideration.

**The Company-PREDICTX**

 PREDICTX is the company under considerations, which is a microfinance company with over 1500 staff. The company has headquarters and branches across other countries. The network and datacenters infrastructure for PREDICTX comprises of hardware and software resources of the entire network connectivity, operations, and communication of an enterprise. Within the network infrastructure, various software that facilitates communication and storage of information is implemented to facilitate communication between users, processes, applications, and external networks (Wangen, 2017). Based on the assessment of PREDICTX company, the application of BizTalk Server to manage communication between internal and external applications requires a comprehensive security assessment to mitigate security threats and vulnerabilities. Deployment of different applications, including in domain controllers, files servers, exchange servers, and print servers, provides storage and sharing of information by the company and access by customers. Additionally, the existence of a firewall within the network and data center architecture provides separation of the network for the organization and external networks.

System vulnerabilities involve weaknesses in system security procedures, design, and implementation of internal security controls. Ideally, assessing security risks is one of the initial steps in evaluating and identifying the risks and consequences of vulnerabilities and security threats (Saleh et al., 2011). In assessing the vulnerabilities within the PREDICTX computer and information systems architecture, security strategies, and policies, it is essential to note that measures put in place are not adequate. Importantly, vulnerability analysis is part of the risk assessment process that focuses on assessing and identifying vulnerability. Agreeably, with risk and security assessment of PREDICTX network infrastructure require mitigating various security vulnerabilities by implementing appropriate protection to safeguard acceptable network security level and protection of information.

Notably, a security framework is meant to provide a holistic platform for security risk analysis against risk and various vulnerability concepts. As provided in the company's case study under consideration, various risks, and security vulnerabilities that can destroy or affect the organization's systems must be looked at and mitigated. Saleh et al. (2011) argue that risk and vulnerabilities are of different forms, e.g., physical risks, natural risks, information, and system security risks. Physical security is meant to protect equipment such as hardware, software systems, and building sites. Considering the physical security of PREDICTX equipment and computer systems, no proper measures have been defined. In terms of natural risks, which include flood, earthquake, fire, among others, have a negative impact on the assets of an organization and the physical structure of an organization. Additionally, the nature of the computer systems and networks may create a loophole for the launching of the attacks from anywhere, making identification of the origin of the attacks to be challenging.

**Risk Determination Overview**

Risk determination is geared towards assessing threats and vulnerabilities to consider their likelihood of occurrence and their consequences in case of their occurrence. Security risk assessment is a mechanism for evaluating security risks that are adopted to identify required security measures. Notably, the risk determination must be conducted in every stage of the system development lifecycle. Similarly, for PREDICTX company that comprises of sensitive information and assets for millions of customers, risk and security assessment is paramount. Risk determination overview for PREDICT company can be described as shown in the table below.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Asset ID | Asset Name | Asset Value | Asset Owner | Threats to Assets | Likelihood Scale |
| 1 | **Exchange Relay Server** | High  | Systems Administrator | * Weak Authentication Procedures
* DoS Attacks
* Data Leakage
* Old and Unnecessary installations
 | Low |
| This is a service primarily used in transporting email messages between different mailing services in different email hosting services, domains, or servers. |
| 2  | **Web Server** | High | Senior Systems Administrator | * Phishing attack
* Misconfiguration attacks
* TCP session hijacking
* Misconfigurations attacks
* Website defacement
 | High  |
| Comprises of software and hardware capable of processing client’s request. Webserver processes incoming network requests using HTTP protocol |
| 3 | **Proxy Server** | High | Network Administrator | * Dynamic content attacks.
* SSL-based DDoS attacks
 | Medium  |
| This basically is another computer which is used as a hub through which processing of internet requests is done |
| 4 | **BizTalk Server** | High | Senior Systems Administrator | * DoS attacks
* Repudiation
* Spoofing Identity
* Malware
 | High  |
| This is a system that organizations to automate business processes by using adaptors tailored to communicate with different applications |
| 5 | **Database Server** | High | Database Administrator | * SQL injection
* Cloud database configuration errors
* Denial of Service
* Exploitation of unpatched services
 | High  |
| Database server is a server that provides data storage services as well as data access |
| 6 | **Exchange Server** | Medium | Network Administrator | * Trojan Horses
* Malware
* Denial of service attacks
 | Medium  |
| An enterprise type of collaboration product that focusses on sending, receiving and storage of email messages |
| 7 | **Firewall** | High | Senior Network Administrator | * Insider attacks
* Missed Security Patches
* DDoS attacks
 | High  |
| A system that is geared towards preventing unauthorized access from private network |
| 8 | **VPN** | High | Senior Network Administrator | * Malware
* DDoS
 | High  |
| It allows creation of secure connection to another network over the internet. |
|  |

|  |  |  |  |
| --- | --- | --- | --- |
| Threats Name | Vulnerability Name | Risk description | Likelihood |
| 1. Poor logical security measures
 | * Lack of proper logical security measures
* No clear definition of data encryption standards
 | The company was not able to devise proper logical control that would involve use of DMZ and IPS to prevent unauthorized access | 5 |
| 1. Poor of physical security
 | Lack of proper physical access control methods such as CCTV and biometric access methods. | The company seems not to have physical restriction methods that would keep track of the movement of people; his is very risky | 4 |
| 1. No email sending policies
 | Ownership and sharing of email issues | The company seems not to have proper mail sending policies, where 2 people can share 1 email accounts | 5 |
| 1. Lack of proper backup mechanisms
 | Redundant servers failing to work  | The company seems not to have effective backup mechanism that would be backing up company data periodically | 4 |

The process of security risk assessment for the organization under consideration involves evaluating and analyzing all assets and processes associated with the system to identify the vulnerabilities and threats, which may have issues in ensuring that there is confidentiality, integrity, and availability of the system, and implementation of acceptable controls to control the risks of assets and information. Assets for PREDICTX include the data centers with application server, web server, Biz Talk server, print server, exchange server, database server, domain controller, custom application server, file server, and client computers. Security risk assessment for the data center and network infrastructure is ideal in identifying security threats and vulnerabilities and identifying proper security controls. In conducting a risk assessment for an organization, risk assessment can be categorized into high-level, comprehensive, and pre-production risk assessment.

The asset value is expensive as it is critical in processing and managing critical information for the organization. Ideally, the most precious aspect is information for the customers and user, which must be protected against information breach and access from unauthorized personnel. High-level risk assessment is applicable at the system design phase to assess and identify possible security risks before implementation. For the case of comprehensive security assessment, it is used in evaluating the security risk of a given system in a department with the aim of providing recommendations for further improvements. Lastly, pre-production assessment is mostly carried out on a new information system or application before it is rolled out for use.

In assessing computer networks, data centers, applications, and all infrastructure of PREDICTX Company as provided, risk assessment of this organization can be viewed in different perspectives. Understandably, infrastructure risk assessment is a security mechanism that involves identifying various risks affecting network infrastructure, technologies, and processes within the organization. The security risk assessment aims at analyzing the large-scale digitization of data and information within the evolution of ubiquitous computing platforms (Tripathy, 2020). Importantly, with IT and network infrastructure, efficiency in service provisioning to the end-users is based on dynamic requirements and security policies put in place by the organization. PREDICTX company appears to be heterogeneous in nature with general-purpose computing systems, communication networks, database management systems, and other software control and application modules.

The possible threats to information and system security of PREDICTX include ineffective security controls, software attacks, sabotage, and information extortion. **Likelihood** of such threats occurring if proper security measures are high. With the implementation of adequate security controls by PREDICTX, likelihood of security threats occurring is very low. Such controls include data encryption, physical security such as use of CCTV, biometric systems, among other controls. Importantly, the first step in security risk assessment is the evaluation and identification of the critical assets and infrastructure for the organization. Based on this assessment, the critical assets for Trip PREDICTX is information being processed on a daily basis, network and data center infrastructure such as web server, exchange relay server, proxy server, file server, BizTalk server, and application server. Security risk assessment for the network and data center also needs to consider looking analyzing and identifying risks linked to a domain controller, database server, exchange server print server, and all computers in the organization. In the web server, security assessment includes checking security controls put in place against possible threats (Verma & Signh, 2013). Ideally, hackers find their way and loopholes to the systems for failure to implement proper security policies. It is worth noting that security controls in the webserver include hardening the server with security policies such as banning the IP addresses that persistently try to access the server without any success.

 The second critical step in security risk assessment, which also out to be applied by the organization in question, is exposure determination. In this phase, what is looked at is the exposure of the entities within the IT infrastructure and systems that may comprise of potential threats and vulnerabilities to various forms of attacks. The primary goal in this step is to report and expose any potential threat by computing the ratio of the potentially unprotected part of the organization's IT infrastructure to the total size of the organization. In exposing possible vulnerabilities and threats within PREDICTX company, the assessment that needs to be done is based on analyzing security controls in place together with possible vulnerabilities available within the organization infrastructure. Such assessment includes evaluating and analyzing different software applications, servers, and the whole network infrastructure, and all the organization assets to identify all the threats. Security risk assessment may be executed by running the server logs for the webserver, database server, application servers, and all other installed components.

 The idea of the fourth step is to collect threat information on each IT entity from internally and externally or from the attackers. With this, it provides guidance on the risk assessment process and identifies appropriate remedial and actions to protect organizational information assets. The fifth step is risk assessment, which aims to identify and measure the degree of the vulnerabilities in the entities, especially in the IT systems. Since all threats do not have equal chances of occurrence and impacts in the organization's infrastructure, it is important for PREDICTX information security specialists to identify various levels of threats. Therefore, each risk level is determined through mapping identified individual threats and vulnerabilities of the organization as per their degree and impacts on the organization's resources that are highly critical. Such assets include the information itself and IT systems.

 The last step is risk mitigation, which involves and acting accordingly by taking preventive measures for potential threats and vulnerabilities with the IT infrastructure. In a similar way, for PREDICTX to be able to maintain the confidentiality, integrity, and availability of its resources, various measures need to be implemented, which include identifying various threats to the company. Other measures include identification of possible threats before their occurrence, mitigating and minimizing of consequences of information and systems security breaches, and finally strategies for recovering to a safe state of the business operations in the event of a crisis.

**Safeguard Determination Phase**

This step involves identifying security controls and safeguarding such controls to safeguard and reduce risk presented by each threat or vulnerability. The 20 Critical Security Controls are designed to help organizations to safeguard their systems and data from attack vectors. Additionally, such controls act as a guideline for the company that do not yet have security programs In this phase safeguard determination involves reducing the risk level of each risk identified from the scenario of PREDICTX. The second step is determining the residual risk likelihood of threat occurrence if the recommended safeguard is implemented. The scenario for PREDICTX can be described using the diagram below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Threats | Recommended Controls and Safeguard | Residual Likelihood of occurrence after the control | Residual Severity of impact after the control | Residual Risk Level after the control |
| No Privacy Policies | -Controlled access-Data protection -No sharing of email accounts - Use of two-factor authentication when logging in to email accounts | Low | Minor | Low |
| Redundant Server Failing to take over | -Proper resynching of data and information periodically-Proper monitoring of the data backups and systems logs-Having Local Server to be backing up server periodically-Data recovery capability | Low | Low | Low |
| Unauthorized person trying to access compound | -Use of CCTV Cameras-Use of Biometric Systems-Boundary defense | Low | Minor | Low |
| Virus threats  | - Using licensed software applications-Regular scanning of computer systems and infrastructure using an effecting anti-virus software.No use of external USB drivers | Low | Minor | Low |
| Hacking attempts | - Use of fail2ban/ win2ban service to block IP addresses trying persistently to scan the server- Definition of firewall rules to prevent attackers from attacking the systems.- Secure Configurations for  | Low | Minor | Low |
| Network Threats | -Use of Secure VPN for communication-continuous vulnerability assessment of networking resources | Low | Minor | Low |
| Unauthenticated Software and hardware configurations  | Secure configurations of hardware and software | Low | Minor | Low |
| Unauthorized access attempts | Maintenance, monitoring, and analysis of audit logs | Low | Minor | Low |
| Malware | Malware defences using appropriate firewall rules and other software packages | Low | Minor | Low |
| Open Network Ports | Limitation and control of network ports | Low | Minor | Low |

The recommended controls and safeguard for PREDICTX IT infrastructure involves implementation of security of policy and architectural parameters within the systems implementation environment. Based on the assessment done, the likelihood occurring assuming the organization embarks on implementing selected safeguard is extremely low. In the fourth step, the goal is to determine possible threats and measuring of **residual risk level** in the organization's assets and information. Residual risk level is specific level of risk after application of security measures. Similarly, residual risk level is the likelihood of occurrence of risks. **The residual risk level** as the PREDICTX IT infrastructure is quite high if proper security controls are not put in place. PREDICTX company needs to identify all the vulnerabilities and threats that may have a direct or indirect impact on the business processes of the organization. Regarding **residual severity,** it is important to note that this is amount of risk or danger related to an action or event remaining after the occurrence of an inherent risk. If the candidate control and inherent and safeguard are implemented in PREDICTX the amount of residual severity would be completely low as such measures would safeguard and provide security control to the IT infrastructure of the organization.

The common vulnerability scoring system is pivotal in the risk assessment of the IT infrastructure of an organization to ensure power and secure information flow across the internal and external systems. The recommended risk assessment modules that PREDICTX needs to consider must apply a data structure known as a vulnerability database. Notably, vulnerability databases can be used in assessing different resources such as network infrastructure, data center infrastructure (webserver, file server, application server, BizTalk server), etc. A vulnerability database is an offline repository stored in the controller, which is always updated periodically with the common vulnerability score values of the applications running and other issues reported recently. Ideally, these values are calculated through the extraction of required metrics from overall vulnerability metrics. The vulnerability values are now available in different formats, such as XML with two different standard scores.

When performing the vulnerability analysis, it is important to consider different assessment parameters such as exploitability group, impact group, attack vector attack complexity, privileges required, remediation level, confidentiality, integrity, and availability. Other key aspects of vulnerability assessment include attack complexity and target distribution (Tripathy, 2020). Information security analysts should be hired to perform tests with the aim of identifying vulnerabilities and providing solutions for maintaining integrity. Arguably, performing penetration testing is a form of vulnerability analysis technique that aims to achieve the following:

1. Risk mitigation and cost related to data recovery in the event of a security attack.
2. Maintaining the integrity of data considered to be highly sensitive within the data center infrastructure. Integrity is a very important aspect of depressing.
3. Improvement of regulatory compliances and applying them for expandability of the entity. Compliances are wide and must be mostly on security.
4. Assessment of the reliability of both software and hardware assets brought from the new vendors.
5. Providing and maintaining confidence to the customers and other users that their personal banking information and transactions are secure.
6. Ensuring that the entity utilizes modern technology and be up to date with the possible tactics employed by the attackers.
7. Identifying unauthenticated and unauthorized services running in the system.
8. Establishment of security information and event management system to record and analyze security logs with the aim of identifying the vulnerabilities within the infrastructure.

Regarding the issue of protecting data for employees, customers, transactions, financial transactions, and other business operations, PREDICTX needs to implement internal and external security controls to guard against fraudulent and unsecure operations. Data protection can also be stored through data encryption, which involves the encryption of emails and other sensitive information. Such data also needs to have backups implemented; this act can act as a disaster recovery plan for the organization under consideration. Implementation of backups for PREDICTX can be implemented either in the cloud architecture or physical backups. Data backups need to be done periodically to ensure that there is the existence of an updated backup copy for the company.

**Conclusion**

 Information security risk assessment is paramount as it helps in assessing potential risks, threats, and vulnerabilities. It is important to perform system security level by identifying potential dangers, threats, or risks associated with the information and systems. In this paper, the goal was to perform a risk assessment for IT infrastructure for PREDICTX company which include data centers with application servers, web servers, database server, BizTalk server, among other important infrastructure. Therefore, performing security assessment is an integral part of organizations' risk management processes and helps in identifying threats and liabilities and solutions to mitigate such threats.

References

Hutter, D. (2016). Physical security and why it is important. *The SANS Institute*.

Kim, J., Yoon, S., Jeong, H., & Won, Y. (2008, December). Implementation and evaluation of a SIP-based secure VoIP communication system. In *2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing* (Vol. 2, pp. 356-360). IEEE.

Lee, K., Oh, I., Lee, Y., Lee, H., Yim, K., & Seo, J. (2018). A study on a secure USB mechanism that prevents the exposure of authentication information for smart human care services. *Journal of Sensors*, *2018*.

Saleh, Z. I., Refai, H., & Mashhour, A. (2011). Proposed Framework for Security Risk Assessment. *J. Information Security*, *2*(2), 85-90.

Tripathy, B. K. (2020). Risk Assessment in IT Infrastructure. In *Ethics, Laws, and Policies for Privacy, Security, and Liability*. IntechOpen.

Verma, S., & Singh, T. (2013). Vulnerability assessment of web servers using honey pots: perspectives, ethical issues, legal implications. *International Journal of Computer Applications*, *72*(22).

Wangen, G. (2017). Information security risk assessment: A method comparison. *Computer*, *50*(4), 52-61.