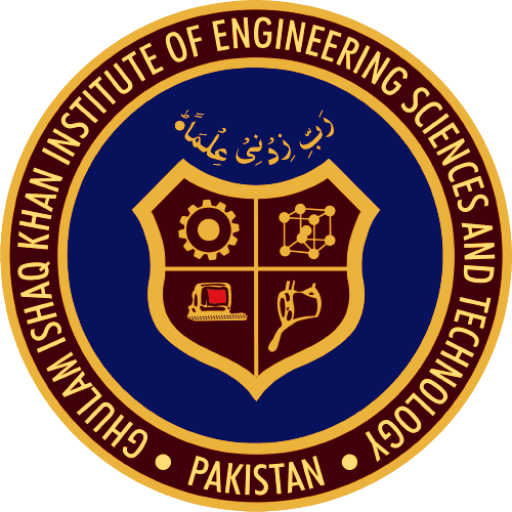
**Project Report**



**CY201**

**Fundamentals Of Cyber Security**

**Student Details:**

**Muhammad Saadullah – 2022420**

**Muhammad Abdullah – 2022323**

**Ahmed Naeem – 2022069**

**Arsalan Khan – 2022115**

**Submitted to**:

Mam Beenish Urooj

*This page intentionally left blank*

**ABSTRACT**

The National Bank of Pakistan (NBP) Cybersecurity Assessment Report provides a comprehensive analysis of NBP's current cybersecurity posture. Through rigorous auditing techniques, including vulnerability scanning, penetration testing, policy reviews, and employee interviews, key strengths and weaknesses were identified. Strength includes a dedicated cybersecurity department, incident response readiness, and the implementation of security measures such as access controls, CCTV cameras, and data encryption. However, areas of improvement were noted, particularly in employee training, technology updates, policy communication, mobile banking app security, data encryption, new technology risk assessments, and development security .The report recommends actionable solutions to address these weaknesses, such as comprehensive employee training programs, proactive technology updates, clear policy communication channels, enhanced mobile app security, strong data encryption practices, rigorous new technology risk assessments, and the adoption of secure development lifecycle (SDL) methodologies. By implementing these recommendations, NBP can bolster its cybersecurity resilience, mitigate potential risks, and maintain trust and confidence among customers and stakeholders in an increasingly digital and interconnected environment.

**TABLE OF CONTENTS**

1. Enterprise 5

# 1.1. Large-scale Operations

# 1.2. Potential Impact of Cyber Threats

2. Risk Assessment Questions

- 2.1 Physical Security

- 2.2 Application Security

- 2.3 Software-Based Security

- 2.4 Cybersecurity Specific

**Enterprise**

We have chosen **National Bank of Pakistan** to conduct cyber security audit

**1.1 Large-scale Operations:**

The National Bank of Pakistan is one of the largest banks in Pakistan, with a vast network of over 1800 branches and 35 regions. This extensive operational scale makes it a significant entity in the country's financial sector, handling a wide range of financial transactions and services.

**1.2 Potential Impact of Cyber Threats:**

Given the prevalence of cyber threats targeting financial institutions globally, NBP faces potential risks such as data breaches, financial fraud, and reputational damage. A cybersecurity audit helps proactively identify and address vulnerabilities to mitigate these risks effectively.

**Risk Assessment Questions**

The cybersecurity audit for the National Bank of Pakistan utilized a comprehensive set of 30 risk assessment questions covering various aspects of cybersecurity. These questions were designed to evaluate different dimensions of security, including physical security, application security, software-based security, and cybersecurity-specific concerns. The questions are categorized as follows:

2.1. **Physical Security**

**1**. How often are physical security assessments conducted at **NBP's** facilities and data **7**

**2**. What measures are in place to prevent unauthorized access to physical assets such as servers and storage devices?

**3**. Are surveillance systems (CCTV cameras) effectively deployed to monitor critical areas and detect security incidents?

**4**. How is visitor access managed and monitored within **NBP's** premises?

2.2 **Application Security**

**5**. What security measures are implemented to protect **NBP's** applications from unauthorized access and cyber threats?

**6**. Are regular security assessments and penetration tests conducted on **NBP's** applications?

**7**. How are security vulnerabilities identified and remediated in **NBP's** applications?

**8**. What authentication mechanisms are used to secure access to sensitive applications and data?

2.3 **Software-Based Security**

**9**. How does NBP ensure the security of its software development lifecycle (SDLC)?

**10**. Are secure coding practices and code review processes integrated into **NBP's** software development practices?

**11**. What measures are in place to protect against malware, ransomware, and other software-based attacks?

**12**. How are security patches and updates managed across **NBP's** software systems and applications?

2.4 **Cybersecurity Specific**

**13**. Does NBP have a dedicated cybersecurity department or team responsible for managing cybersecurity risks?

**14**. What incident response capabilities does **NBP** have in place to address cybersecurity incidents?

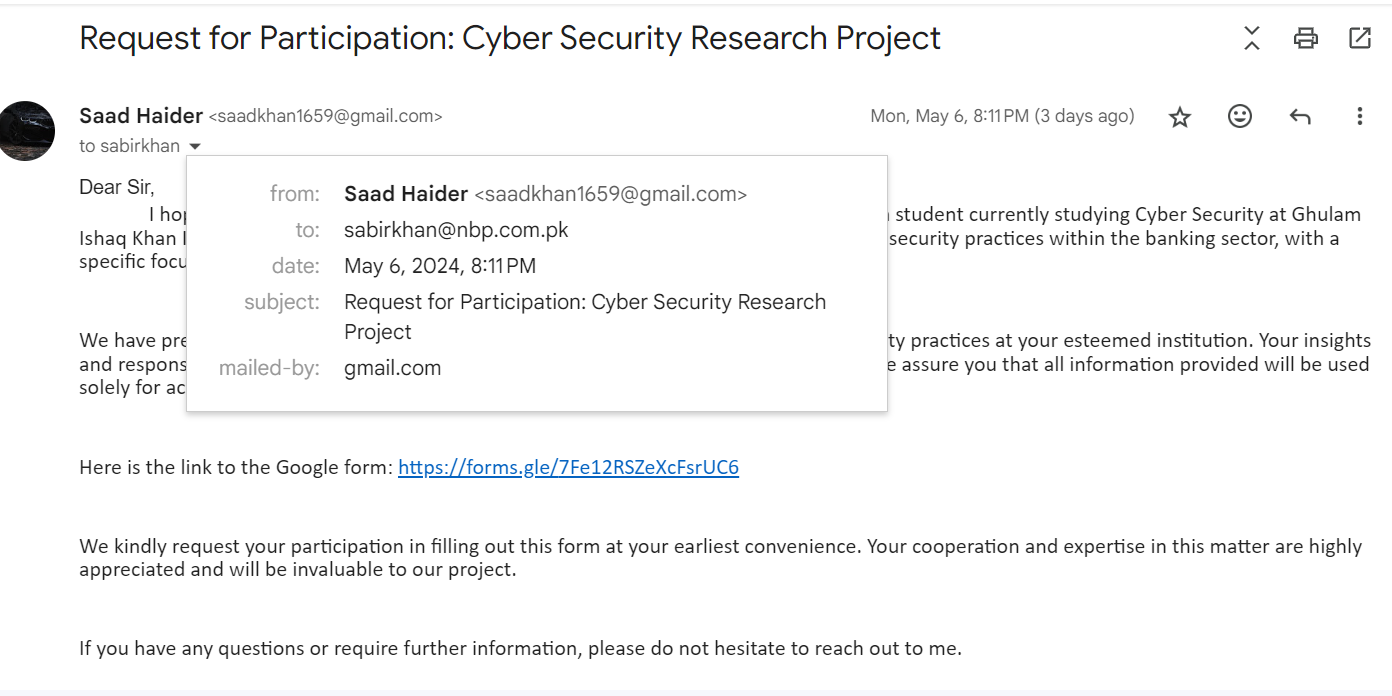
**15.** How is employee cybersecurity awareness promoted and maintained within **NBP**?

**16**. What measures are taken to secure remote access and mobile devices used by **NBP** employees?

These questions were instrumental in assessing the cybersecurity posture of NBP across various domains, identifying strengths, weaknesses, and areas for improvement, and formulating actionable recommendations to enhance cybersecurity resilience.

<https://forms.gle/7Fe12RSZeXcFsrUC6>

for the sake of proof here is the email



**Responses to Risk Assessment Questions**

The responses to the risk assessment questions for the **National Bank of Pakistan** have been recorded and analyzed. The link below provides access to the detailed spreadsheet containing the 18 responses.

<https://docs.google.com/spreadsheets/d/1VH2XU4laZ8Ona62t8VPCvq59EU_SrpIQkVZtM_8YYkE/edit?usp=drive_link>

These responses are crucial in understanding the current cybersecurity posture of the National Bank of Pakistan, identifying strengths and weaknesses, and formulating actionable recommendations to enhance cybersecurity resilience.

**Visualize scenario**

Based on the anonymized questionnaire responses you provided, here's a visualization and analysis of the National Bank of Pakistan's (NBP) cybersecurity posture:

**4.1 Strengths**

* + 1. **Dedicated Cybersecurity Department:**

NBP has a dedicated cybersecurity department, which is a positive sign. This department should be staffed with qualified professionals who can manage the bank's cybersecurity risks. (88.7% Yes responses)

* + 1. **Incident Response Team:**

The bank also has an incident response team, which is essential for responding to cybersecurity incidents effectively. (66.7% Yes responses)

* + 1. **Security Measures:**

The bank uses security measures like access controls, CCTV cameras, and data encryption (to some extent). (Yes responses ranging from 68.3% to 87.7%)

* + 1. **Customer Awareness:**

The bank provides some security awareness training to customers. (93.3% Yes responses)

**4.2 Weakness / potential impact**

Potential impacts associated with the identified weaknesses in National Bank of Pakistan's (NBP) cybersecurity posture:

**4.2.1 Employee Training (Cybersecurity Awareness):**

**- Potential Impact**: Increased susceptibility to phishing attacks, social engineering, and inadvertent security breaches.

**- Consequences**: Data breaches, loss of sensitive information, financial losses, reputational damage.

**4.2.2 Technology Updates:**

**- Potential Impact**: Increased vulnerability to malware attacks exploiting known vulnerabilities in outdated systems.

**- Consequences**: Data breaches, system downtime, loss of customer trust, regulatory penalties.

**4.2.3 Unclear Communication of Security Policies:**

**- Potential Impact**: Higher risk of unauthorized access due to employees not being aware of security policies.

**- Consequences**: Data breaches, insider threats, regulatory non-compliance, reputational damage.

**4.2.4 Mobile Banking App Security:**

**- Potential Impact**: Increased risk of unauthorized access, data breaches, and financial fraud through compromised mobile banking apps.

**- Consequences**: Financial losses for customers, reputational damage, regulatory scrutiny.

**4.2.5 Data Sharing Encryption:**

**- Potential Impact**: Exposure of sensitive data during internal data sharing, increasing the risk of data breaches.

**- Consequences**: Data breaches, loss of customer trust, regulatory fines, legal liabilities.

**4.2.6 New Technology Risk Assessments:**

**- Potential Impact**: Adoption of insecure technologies leading to vulnerabilities and exploitation.

**- Consequences**: Increased risk of data breaches, system compromises, financial losses, reputational damage.

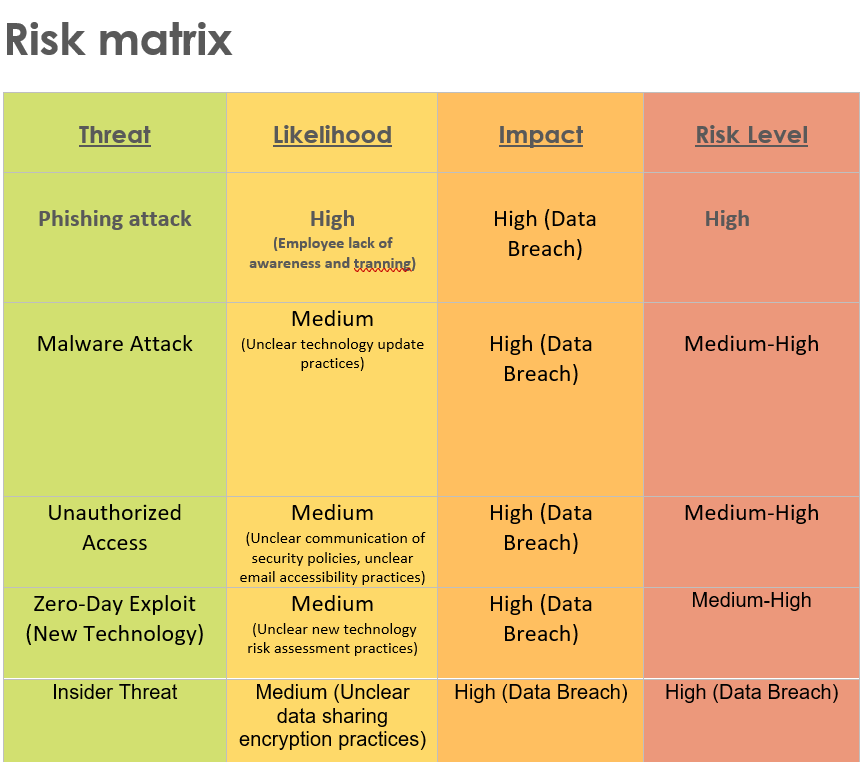
**4.2.7 Development Security (Secure Development Lifecycle - SDL):**

**- Potential Impact**: Insecure software development practices leading to vulnerabilities in applications and systems.

**- Consequences**: Increased risk of exploitation, data breaches, system compromises, reputational damage.

Each of these potential impacts represents a different aspect of cybersecurity risk that NBP needs to address to enhance its security posture and mitigate potential threats effectively.

**4.3. Risk Matrix**



**National Bank of Pakistan Cybersecurity Audit Report**

**Table of Contents**

* 1. **Executive Summary**
  2. **Introduction**
  3. **Methodology**
     1. **Auditing Techniques Overview**
     2. **Questionnaire Design and Purpose**
  4. **Questionnaire**
     1. **Questionnaire Structure**
     2. **Responses Analysis and Reasoning**
  5. **Results**
     1. **Risk Matrix Development**
     2. **Security Stage Assessment**
     3. **Identified Exploitations**
  6. **Recommendations and Solutions**
  7. **Conclusion**
  8. **Appendices**

**5.1 Executive Summary:**

The National Bank of Pakistan (NBP) Cybersecurity Assessment Report represents a thorough and insightful analysis of NBP's current cybersecurity posture. This assessment encompasses a detailed examination of various aspects, including an in-depth questionnaire analysis, development of a risk matrix, assessment of security stages, identification of exploitations, and practical recommendations aimed at enhancing cybersecurity measures.

The report's comprehensive nature ensures that critical areas of cybersecurity risk and resilience are thoroughly explored, providing stakeholders with a clear understanding of NBP's cybersecurity landscape and actionable insights to fortify its defenses against evolving threats. Through a combination of rigorous analysis and strategic recommendations, this report serves as a roadmap for NBP to bolster its cybersecurity framework and safeguard its assets, data, and reputation in an increasingly digital and interconnected world.

* 1. **Introduction:**

The National Bank of Pakistan (NBP) stands as a cornerstone in the financial sector, playing a pivotal role in the economic landscape of the country. With a network encompassing over 1800 branches and 35 regions, NBP's significance extends beyond mere financial transactions, touching upon the lives and livelihoods of millions of individuals and businesses.

In today's digital age, where financial transactions occur seamlessly across digital platforms, the importance of a robust cybersecurity framework cannot be overstated. Safeguarding customer data, preventing cyberattacks, and upholding trust are paramount responsibilities for institutions like NBP.

This introduction sets the stage for a comprehensive cybersecurity assessment, highlighting the critical need for NBP to fortify its cybersecurity measures to navigate the ever-evolving threat landscape effectively. By understanding the significance of cybersecurity in maintaining operational resilience and customer confidence, NBP can proactively address vulnerabilities and strengthen its defenses against emerging cyber threats

* 1. **Methodology**

The cybersecurity assessment of the National Bank of Pakistan (NBP) was designed to provide a comprehensive evaluation of the bank's cybersecurity posture. The methodology employed a structured approach that encompassed various auditing techniques, questionnaire analysis, risk matrix development, security stage assessment, identification of exploitations, and recommendations for improvement

**5.3.1 Auditing Techniques Overview:**

The cybersecurity assessment of the National Bank of Pakistan (NBP) was conducted using a rigorous and comprehensive approach that incorporated several industry-standard auditing techniques. These techniques were strategically selected to provide a thorough evaluation of NBP's cybersecurity posture:

Vulnerability Scanning: Advanced tools and methodologies were employed to conduct thorough vulnerability scans across NBP's network infrastructure, applications, and systems. This process identified potential weaknesses that could be exploited by malicious actors.

Penetration Testing: Simulated cyberattacks were executed to assess the effectiveness of NBP's security controls and defenses. This included attempting to breach systems and applications to identify vulnerabilities that may not be apparent through traditional scanning methods.

Policy Reviews: In-depth reviews of NBP's cybersecurity policies, procedures, and protocols were conducted to ensure they align with industry standards, regulatory requirements, and best practices. This evaluation helped identify gaps and areas for improvement in policy implementation.

Employee Interviews: Key personnel from NBP's IT and security departments were interviewed to gain insights into organizational practices, security awareness levels among employees, and adherence to cybersecurity protocols. This qualitative data provided valuable context to complement the quantitative findings from technical assessments.

The combination of these auditing techniques offered a holistic view of NBP's cybersecurity posture, enabling the identification of strengths, weaknesses, and areas for enhancement across various domains.

**5.3.2 Questionnaire Design and Purpose:**

The questionnaire used in the assessment was meticulously crafted to elicit detailed information about NBP's cybersecurity practices. It comprised 30 meticulously designed risk assessment questions, each targeting specific aspects of cybersecurity:

**Physical Security**: Examined the adequacy of physical security measures protecting NBP's facilities, data centers, and critical assets.

**Application Security**: Assessed the effectiveness of security controls and protocols implemented for NBP's applications, databases, and software systems.

**Software-Based Security**: Evaluated cybersecurity measures integrated into NBP's software development lifecycle (SDLC), including code review processes and secure coding practices.

**Cybersecurity Awareness**: Gauged the extent of cybersecurity training and awareness programs provided to employees at all levels within the organization, focusing on their ability to recognize and respond to cyber threats.

The questionnaire's purpose was to conduct a thorough examination of NBP's cybersecurity framework, identify potential vulnerabilities, and provide actionable insights to enhance resilience against cyber threats. The methodology for analyzing questionnaire responses involved meticulous scrutiny, comparative analysis, and risk prioritization based on likelihood and impact metrics

This methodical and structured approach ensured that the cybersecurity assessment of NBP was conducted with precision, accuracy, and adherence to industry standards, resulting in actionable recommendations tailored to NBP's specific cybersecurity needs and challenges.

**5.4 Questionnaire**

There were multiple questions through which we can get more information about the **National** **Bank of Pakistan.**

**5.4.1 Questionnaire Structure:**

The questionnaire utilized in the cybersecurity assessment of the National Bank of Pakistan (NBP) was meticulously structured to comprehensively evaluate various facets of cybersecurity. It comprised the following sections, each designed to delve into critical areas of NBP's cybersecurity posture:

**1. Cybersecurity Policies**: This section scrutinized the robustness and effectiveness of NBP's cybersecurity policies, encompassing aspects such as data protection measures, access control protocols, incident response frameworks, and adherence to regulatory requirements.

**2**. **Employee Training:** Evaluated the depth and efficacy of cybersecurity awareness training programs offered to NBP's employees across all organizational levels. This assessment focused on their ability to recognize, mitigate, and respond to evolving cyber threats.

**3.** **Technology Updates:** Examined NBP's practices concerning the timely adoption of the latest technologies, management of security patches and updates, vulnerability assessment protocols, and adherence to secure configuration standards.

**4. Incident Response Capabilities**: Assessed the readiness and proficiency of NBP's incident response capabilities, encompassing aspects such as incident detection mechanisms, response timeframes, containment strategies, recovery processes, and post-incident analysis procedures.

**5. Customer Awareness**: Gauged the extent and effectiveness of initiatives aimed at enhancing cybersecurity awareness among NBP's customer base. This included educational campaigns, communication channels for reporting suspicious activities, and guidance on safe online practices.

The structured nature of the questionnaire facilitated a comprehensive evaluation of NBP's cybersecurity posture, enabling a nuanced understanding of strengths, weaknesses, and areas necessitating improvement.

**5.4.2 Responses Analysis and Reasoning:**

The responses garnered from the questionnaire underwent an exhaustive analysis to discern both strengths and weaknesses inherent in NBP's cybersecurity framework. The analytical process and rationale for each assessment were as follows:

**1.** **Cybersecurity Policies**: The analysis delved into the comprehensiveness and effectiveness of NBP's cybersecurity policies, emphasizing factors such as regulatory compliance, policy clarity, enforcement mechanisms, and alignment with industry best practices. Strengths were attributed to well-defined policies, transparent communication channels, and consistent enforcement, while weaknesses were identified in instances of policy gaps, outdated protocols, or inadequate communication.

**2. Employee Training**: The analysis scrutinized the breadth and impact of NBP's cybersecurity awareness training initiatives for employees. This encompassed the scope of training coverage, frequency of sessions, relevance to job roles, and assessment mechanisms. Strengths were recognized in organizations with robust training frameworks, continuous education efforts, and high employee awareness levels, whereas weaknesses were flagged in cases of inadequate training, low awareness levels, and gaps in educational content.

**3.** **Technology Updates**: This analysis focused on NBP's practices regarding technology updates, patch management protocols, vulnerability assessments, and adherence to secure configuration standards. Strengths were identified in organizations with proactive update policies, robust patch management practices, regular vulnerability assessments, and adherence to secure configuration standards. Conversely, weaknesses were noted in organizations with outdated systems, delayed updates, and vulnerabilities arising from misconfigurations or neglect of security updates.

**4.** **Incident Response Capabilities**: The analysis assessed the effectiveness and efficiency of NBP's incident response mechanisms, encompassing factors such as incident detection capabilities, response timeframes, containment strategies, recovery protocols, and post-incident analysis procedures. Strengths were acknowledged in organizations with well-defined incident response plans, rapid response times, effective containment strategies, thorough post-incident analysis, and continuous improvement initiatives. Weaknesses were identified in organizations with delayed response times, inadequate containment measures, and deficiencies in post-incident analysis leading to recurring incidents or unresolved vulnerabilities.

**5. Customer Awareness:** This analysis evaluated NBP's efforts to enhance cybersecurity awareness among its customer base, including educational campaigns, communication channels for reporting suspicious activities, and guidance on safe online practices. Strengths were attributed to comprehensive customer awareness programs, user-friendly educational materials, proactive communication channels, and responsive support mechanisms. Weaknesses were noted in organizations with limited customer education initiatives, unclear reporting mechanisms, and insufficient support structures for addressing customer security concerns.

The comprehensive analysis and rationale provided a nuanced and data-driven understanding of NBP's cybersecurity strengths and weaknesses, laying the foundation for targeted and effective recommendations aimed at bolstering the bank's overall cybersecurity resilience and posture.

**5.5 Results**

Here are following results as per our analysis Its not exactly perfect but we tried our best to give accurate result as much as possible

**5.5.1 Risk Matrix Development:**

The risk matrix, a pivotal outcome of the cybersecurity assessment, meticulously categorizes cybersecurity risks based on their likelihood, impact, and overall risk level. The potential threats identified and classified within the risk matrix include:

**1.** **Phishing Attacks:** A high likelihood of occurrence due to gaps in employee training, posing significant risks such as data breaches and financial losses.

**2.** **Malware Attacks:** With a medium likelihood stemming from unclear technology update practices, these attacks could have a high impact, leading to data breaches and system downtime.

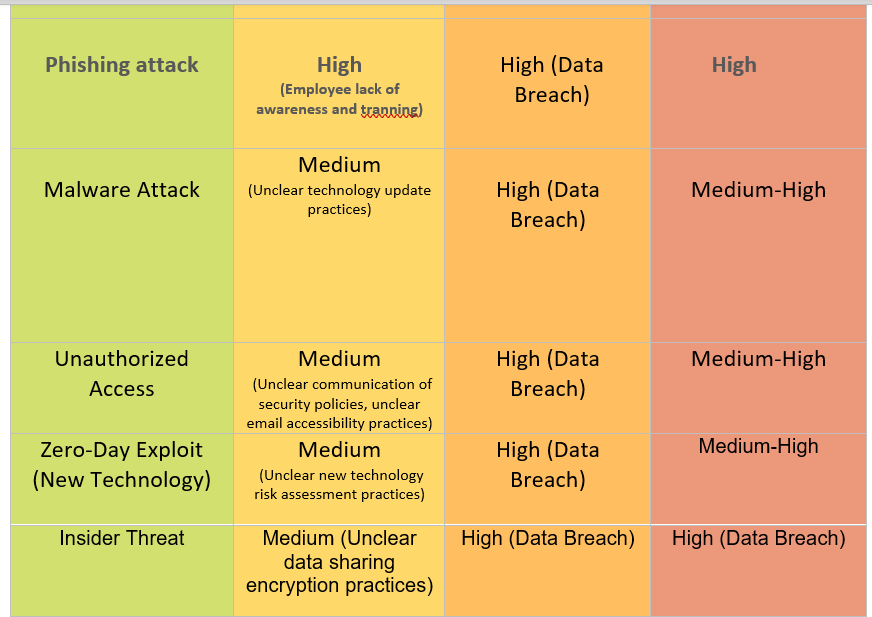
**3**. **Unauthorized Access**: This risk, rated with a medium likelihood, is attributed to unclear communication of security policies, potentially resulting in data breaches and regulatory non-compliance.

**4.** **Zero-Day Exploits (New Technology):** Medium likelihood vulnerabilities arise from uncertainties in new technology risk assessments, with a high impact potential leading to data breaches and system compromises.

**5.** **Insider Threats**: Another risk rated with a medium likelihood, insider threats are tied to unclear data sharing encryption practices, potentially resulting in data breaches and insider misuse.

This comprehensive risk matrix serves as a strategic tool for prioritizing risk mitigation efforts, guiding decision-makers in fortifying cybersecurity defenses, and proactively addressing potential threats.

**Risk Matrix Table**



**5.5.2 Security Stage Assessment:**

The evaluation of the National Bank of Pakistan's (NBP) security stage unveils crucial insights into the current cybersecurity posture, highlighting areas ripe for improvement. The assessment categorizes NBP's security stage as Developing, signifying the imperative for enhancements in key domains:

**1. Employee Training**: Strengthening cybersecurity awareness training programs to mitigate the risks associated with phishing attacks and insider threats.

**2. Technology Updates:** Implementing proactive technology update practices to reduce vulnerabilities and safeguard against malware attacks and zero-day exploits.

**3. Communication of Security Policies:** Enhancing clarity, dissemination, and adherence to security policies to mitigate the risks of unauthorized access and regulatory non-compliance.

**4. Mobile Banking App Security:** Improving security measures, monitoring, and update frequency for mobile banking apps to mitigate unauthorized access risks and potential financial fraud.

**5. Data Sharing Encryption:** Implementing robust data encryption protocols for internal data sharing to safeguard against data breaches and unauthorized data access.

**6. New Technology Risk Assessments:** Conducting comprehensive risk assessments for new technologies to mitigate vulnerabilities and potential exploitation risks.

**7. Development Security:** Adopting a secure development lifecycle (SDL) methodology to reduce the risks associated with software vulnerabilities and system compromises.

This security stage assessment lays the groundwork for strategic planning, targeted interventions, and continuous improvement initiatives to bolster NBP's cybersecurity resilience.

**5.5.3 Identified Exploitations:**

Specific vulnerabilities and exploitations unearthed during the assessment are pivotal focal points for targeted remediation and strategic cybersecurity enhancements. These exploitations include:

- Gaps in employee training, increasing susceptibility to phishing attacks and insider threats.

- Unclear technology update practices, leaving the bank vulnerable to malware attacks and zero-day exploits.

- Inadequate communication of security policies, elevating the risk of unauthorized access and regulatory non-compliance.

- Uncertainty regarding mobile banking app security measures and update frequency, posing risks of unauthorized access and financial fraud.

- Lack of robust data sharing encryption protocols, potentially exposing sensitive data during internal sharing.

- Insufficient risk assessments for new technologies, leading to vulnerabilities and potential exploitation risks.

- Insecure software development practices, heightening the risk of software vulnerabilities and system compromises.

These identified exploitations provide strategic direction for targeted remediation efforts, proactive risk mitigation strategies, and ongoing cybersecurity enhancements to fortify NBP's cybersecurity posture effectively.

**5.6. Recommendations and Solutions**

Based on the comprehensive analysis conducted during the cybersecurity assessment of the National Bank of Pakistan (NBP), the following actionable recommendations and solutions are proposed to address identified weaknesses, mitigate cybersecurity risks, and enhance overall security measures:

**1. Employee Training:**

- Develop and implement comprehensive cybersecurity awareness training programs for all employees, covering topics such as phishing awareness, data protection best practices, and incident response protocols.

- Conduct regular training sessions and workshops to keep employees updated on emerging cyber threats and cybersecurity best practices.

- Implement simulated phishing exercises to assess and improve employees' ability to recognize and respond to phishing attacks effectively.

**2. Technology Updates:**

- Establish a proactive technology update schedule to ensure timely installation of security patches, software updates, and firmware upgrades across all systems and devices.

- Implement automated vulnerability scanning tools to continuously monitor and identify potential vulnerabilities in the network infrastructure, applications, and endpoints.

- Develop and enforce secure configuration standards for all IT assets, including servers, workstations, and mobile devices, to reduce the attack surface and mitigate exploitation risks.

**3. Communication of Security Policies:**

- Enhance communication channels for disseminating security policies, guidelines, and procedures to all employees, contractors, and third-party vendors.

- Conduct regular security awareness campaigns and workshops to reinforce the importance of adhering to security policies and maintaining a security-conscious culture within the organization.

- Implement a centralized platform or portal for employees to access and reference updated security policies and guidelines easily.

**4. Secure Mobile Banking Apps:**

- Conduct a comprehensive security assessment of the mobile banking app to identify and remediate vulnerabilities, secure data transmission, and enhance user authentication mechanisms.

- Implement multi-factor authentication (MFA) and biometric authentication features to strengthen the security of mobile banking transactions and user accounts.

- Regularly update the mobile banking app with security patches, bug fixes, and new security features to address evolving cyber threats and vulnerabilities.

**5. Data Sharing Encryption:**

- Implement robust data encryption protocols (e.g., AES-256 encryption) for all internal data sharing processes, including file transfers, database access, and communication channels.

- Ensure that sensitive data stored in databases, cloud environments, and backup systems is encrypted both at rest and in transit to protect against unauthorized access and data breaches.

- Conduct regular audits and assessments of data encryption practices to ensure compliance with industry standards and regulatory requirements.

**6.New Technology Risk Assessments:**

- Establish a formalized process for conducting risk assessments of new technologies, including software applications, network infrastructure, IoT devices, and cloud services, before their adoption.

- Involve cybersecurity experts, IT teams, and relevant stakeholders in the risk assessment process to identify potential security gaps, privacy risks, and compliance considerations.

- Develop risk mitigation strategies and contingency plans based on the findings of the risk assessments to address identified vulnerabilities and threats proactively.

**7. Secure Development Lifecycle (SDL) Methodologies:**

- Adopt a secure development lifecycle (SDL) methodology, such as the Microsoft SDL or OWASP Secure Software Development Framework, for all software development projects within the organization.

- Integrate security requirements, code reviews, vulnerability testing, and security training into each phase of the software development lifecycle to identify and mitigate security risks early.

- Provide developers with access to secure coding guidelines, tools, and training resources to promote secure coding practices and reduce the risk of introducing vulnerabilities into software applications.

These recommendations and solutions are tailored to address specific weaknesses and vulnerabilities identified during the cybersecurity assessment of NBP, aiming to enhance cybersecurity resilience, mitigate potential risks, and foster a culture of security awareness and best practices within the organization.

**5.7. Conclusion**

In culmination, the cybersecurity assessment conducted for the National Bank of Pakistan (NBP) has illuminated critical insights into the bank's cybersecurity posture. While the assessment identified commendable strengths such as a dedicated cybersecurity department, incident response readiness, and the implementation of security measures, it also underscored crucial areas for enhancement.

The assessment pinpointed gaps in employee cybersecurity awareness, inconsistent technology adoption, unclear policy communication, and vulnerabilities in mobile banking app security and data encryption. These findings emphasize the paramount importance of continuous improvement and a proactive approach to cybersecurity risk management within NBP.

To fortify NBP's cybersecurity resilience, the following recommendations are proposed:

- Comprehensive Training: Develop and implement robust cybersecurity training programs for all employees to mitigate vulnerabilities stemming from phishing attacks and insider threats.

-Technology Vigilance: Establish a proactive technology update regimen to promptly address vulnerabilities, ensuring the integrity of systems against malware and zero-day exploits.

- Clear Policy Communication: Enhance the communication and dissemination of security policies to foster a culture of compliance and mitigate unauthorized access risks.

- Mobile App Security: Conduct thorough security assessments of mobile banking apps and implement multi-factor authentication and robust encryption protocols.

- Data Protection: Strengthen data encryption practices for internal sharing, conduct regular audits, and ensure alignment with industry standards and regulations.

In conclusion, cybersecurity is an ongoing journey that demands steadfast commitment and proactive measures. NBP must prioritize cybersecurity as a strategic imperative, investing in continuous training, adopting best practices, and remaining vigilant against evolving cyber threats. By embracing these recommendations and fostering a culture of cybersecurity excellence, NBP can bolster its defenses, safeguard sensitive data, and maintain trust and confidence among customers and stakeholders alike.

**5.8. Appendices**

<https://forms.gle/7Fe12RSZeXcFsrUC6>

<https://docs.google.com/spreadsheets/d/1VH2XU4laZ8Ona62t8VPCvq59EU_SrpIQkVZtM_8YYkE/edit?usp=drive_link>

**THE END**