## Slide 1:

Hello everyone, my name is Ritesh, and I am here with my team members Pooja, Ezhil, Pritam, and Sowjanya. Today, we will provide an overview of FinTrust Inc. and present the roadmap of our customized Zero Trust assessment for FinTrust.

## Slide 2:

We will explore the impact of cybersecurity breaches, particularly in the financial sector, and outline our customized Zero Trust assessment to enhance our security framework. We will explain the Six Pillars of Zero Trust and the Zero Trust Maturity Model, identify gaps in our current security posture, and present a detailed roadmap to address these vulnerabilities.

## Slide 3:

FinTrust Inc. was founded in 1998 in New York City and has become a leading financial services provider. Our services include online banking, investment management, and personalized financial advisory. With over 700 employees, we serve 1.2 million clients and generate $250 million in annual revenue.

## Slide 4:

The concept of Zero Trust is defined by the National Institute of Standards and Technology (NIST) in Special Publication 800-207. The primary goal of Zero Trust is to prevent unauthorized access to data and services while making access control enforcement as granular as possible.

The Zero Trust model is built on the principle of "never trust, always verify." This means that no one is trusted by default from inside or outside the network, and verification is required from everyone trying to access resources on the network.

## Slide 5:

The Six Pillars of Zero Trust provide a robust framework for securing our digital infrastructure and services:

1. Identities: Ensure strong authentication for all users, verifying their legitimacy before granting access.

2. Devices: Monitor and enforce the health and compliance of all devices accessing the system.

3. Apps and APIs: Ensure applications and APIs have secure configurations and appropriate permissions.

4. Data: Classify and protect data with necessary attributes and encryption.

5. Infrastructure: Harden both on-premises and cloud infrastructure against potential attacks.

6. Networks: Segment, monitor, analyze, and encrypt network traffic to control access and identify threats.

## Slide 6:

Data breaches have significant consequences for financial institutions. A recent breach at a competitor bank affected over 300,000 customers, leading to millions in financial losses and severe reputational damage. Such incidents result in a decline in customer confidence, highlighting the urgency for robust cybersecurity.

Implementing strong security measures, like the Zero Trust framework, protects customer data and maintains trust.

## Slide 7:

Our assessment approach for implementing Zero Trust at FinTrust involves several key steps to ensure a comprehensive and tailored evaluation of our security posture.

1. Assessment with Zero Trust Maturity Model: We will conduct a detailed evaluation of FinTrust's current security strengths and weaknesses using the Zero Trust Maturity Model.

2. Customization for FinTrust's Environment: The assessment will be tailored specifically to FinTrust's operational needs.

3. Diverse User Group Considerations: We will implement role-based access controls to cater to the diverse user groups within our organization.

4. Complex Device Management: Given the variety of devices used within FinTrust, we will strategize for a mixed device ecosystem.

## Slide 8:

The CISA Zero Trust Maturity Model outlines four stages in the journey toward achieving a fully integrated Zero Trust environment.

1. Optimal Stage: At this stage, an organization has a fully integrated Zero Trust environment with advanced security measures in place.

2. Advanced Stage: This stage involves extensive automation and coordination across the organization.

3. Initial Stage: Organizations at this stage have basic automation and visibility.

4. Traditional Stage: This is the current state for FinTrust. At this stage, there is limited automation and visibility, and the organization relies on basic security controls. This stage represents the starting point for our Zero Trust journey.

Our goal is to move from the Traditional Stage to the Optimal Stage by gradually implementing the necessary security measures and automation.

## Slide 9:

Our assessment identified two key issues in People/Identity:

1. Weak Password Policies: Infrequent password changes increase the risk of exploitation.
2. Limited MFA Implementation: The lack of Multi-Factor Authentication (MFA) exposes accounts to unauthorized access.

## Slide 10:

Our assessment identified critical gaps in the Devices dimension:

1. Inconsistent Management of Personal Devices: Access to customer data through personal devices lacks uniformity, increasing security risks.

2. Security Protocols for IoT Devices: The absence of specific security protocols for IoT devices can lead to potential vulnerabilities.

## Slide 11:

Our assessment identified two major gaps in the Applications dimension:

1. Patch Management Inefficiencies: The processes for updating and patching financial applications are often slow or ineffective. This can leave applications vulnerable to known exploits.

2. Vulnerabilities in Default Configurations: Applications might be easily exploited due to default settings that are not sufficiently secure.

## Slide 12

Our evaluation has revealed two significant weaknesses in the Data dimension:

1. Inconsistent Data Classification: The lack of consistent data classification practices may result in insufficient security for sensitive data.

2. Data Encryption Absence: The absence of data encryption increases the risk of exposing customer data during breaches.

Addressing these gaps will enhance our data security, ensuring that sensitive information is adequately protected and reducing the risk of data breaches.

## Slide 13

Our evaluation has revealed two critical weaknesses in the Network dimension:

1. Flat Network Structure Vulnerabilities: A flat network structure allows attackers to move laterally within the network, potentially enabling unauthorized access to sensitive data.

2. Network Segmentation Deficiencies: Insufficient network segmentation leaves critical systems unprotected, increasing the risk of exposure to attacks.

## Slide 14

Our evaluation has highlighted two significant gaps in the Infrastructure dimension:

1. Limited Security Automation Tool Usage: The lack of automation tools hampers efficient threat detection and slows down the response to security incidents.

2. Absence of Centralized Security Information and Event Management (SIEM) System: Without a centralized SIEM system, correlating security events from different sources is challenging. This makes it difficult to manage and respond to security incidents effectively.

## Slide 15

To enhance our People/Identity security, we will focus on three key areas:

1. Strong Password Policies: Enforce regular password changes, such as every 90 days, to minimize the risk of compromised passwords.

2. Multi-Factor Authentication (MFA): Deploy MFA for all user accounts to provide an additional layer of security, making it harder for unauthorized users to gain access.

3. Biometric Authentication: Assess the use of biometric authentication for secure access points, further enhancing security by leveraging unique physical traits.

## Slide 16

To improve device security, we will focus on the following areas:

1. Device Management Policy Development: Enforce the use of bank-issued devices for staff handling sensitive data to ensure consistent security standards.

2. Endpoint Detection and Response (EDR) Implementation: Deploy EDR solutions across all devices to monitor and mitigate threats in real-time, enhancing our ability to respond to security incidents.

3. IoT Device Security Protocols: Establish strict guidelines for securing and managing IoT devices within the network, ensuring that these devices do not become weak points in our security infrastructure.

## Slide 17

To enhance application security, we will focus on the following areas:

1. Regular Vulnerability Assessments: Perform consistent checks and updates for financial applications to identify and address vulnerabilities promptly.

2. Least Privilege Access Controls: Grant minimal permissions necessary for application functions, ensuring that users have only the access they need to perform their tasks.

3. Application Whitelisting Enforcement: Restrict usage to authorized software only, preventing the installation and execution of unauthorized applications.

## Slide 18

To improve data security, we will focus on the following areas:

1. Data Classification Framework: Categorize customer data based on sensitivity levels to ensure appropriate protection measures are in place for different types of data.

2. Data Encryption Measures: Encrypt data at rest and during transit to maintain confidentiality and protect sensitive information from unauthorized access.

3. Data Loss Prevention (DLP) Deployment: Implement DLP solutions to detect and block unauthorized data leaks, ensuring sensitive information remains secure.

## Slide 19

To enhance our infrastructure security, we will focus on the following areas:

1. Centralized Log Collection and Analysis: Use SIEM tools for efficient log management and to improve our ability to detect and respond to security incidents.

2. Security Process Automation: Implement automation to reduce errors, streamline security processes, and enhance overall efficiency.

3. Threat Intelligence Integration: Incorporate threat intelligence feeds to stay updated on the latest threats and improve our proactive security measures.

## Slide 20:

To enhance network security, we will focus on the following areas:

1. Network Segmentation for Customer Data Protection: Isolate critical systems containing sensitive customer information to limit access and reduce the risk of unauthorized access.

2. Access Control Implementation: Enforce restrictions to prevent unauthorized network movement, ensuring that users can only access the parts of the network necessary for their roles.

3. Advanced Network Monitoring: Improve detection of suspicious activities and potential security breaches by implementing advanced monitoring tools and techniques.

## Slide 21:

Building a robust culture of security within FinTrust is essential for maintaining customer and stakeholder trust. Here are the key elements we need to focus on:

1. Building Trust with Cybersecurity: A strong cybersecurity posture is crucial for building and maintaining trust with our customers and stakeholders.

2. Cultural Shift in Security: Security goes beyond technical measures; it requires a cultural shift within the organization. We need to foster a security-first mindset among all employees, ensuring that everyone understands their role in maintaining security.

3. Ongoing Security Process: Continuous monitoring and adaptation are vital to stay ahead of evolving cyber threats. Regular security drills and integrating threat intelligence feeds are necessary to test our defenses and update our strategies.

4. Shared Responsibility for Security: Security is a shared responsibility. We must encourage open communication about security issues and promote a culture where employees feel comfortable reporting suspicious activities.

## Slide 22:

To ensure a secure future, we will take the following steps:

1. Detailed Implementation Plan: Develop a comprehensive plan with timelines and budget considerations, breaking down the process into manageable phases for a smooth transition.

2. Ownership and Accountability: Assign specific teams or individuals for each action item to ensure clear leadership and accountability throughout the implementation.

3. Stakeholder Engagement: Emphasize the importance of communication with stakeholders by scheduling regular update meetings to keep everyone informed and involved.

4. Ongoing Support for FinTrust: Provide access to security consultants and offer additional training programs to support our team as we implement these changes.

In conclusion, our commitment to enhancing cybersecurity through the adoption of the Zero Trust framework is not just about compliance but about fostering a culture of security that permeates every aspect of our operations. Zero Trust principles—never trust, always verify—will guide us in securing our infrastructure, protecting our data, and ensuring that only authorized individuals have access to our systems.

## Slide 23

We extensively referred to these documents while creating this presentation.

## Slide 24

Thank you. That concludes our presentation.