Digital Trust Assessment

Michigan Avenue Fitness Center

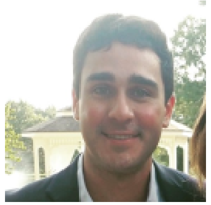
Patrick Eckland, Satvik Yagnamurthy, Yemi Adetutu, Yinwei Wang, Jamia Russell

10/27/2024

Presentation Agenda

- □ Team Profile
- □ Company Overview
- □ Assessment Approach: Zero Trust Framewor
- □ Maturity Model
- □ Current State Assessment
- □ Pain Points
- □ Next Steps - Implementation Plan

Team Profile



Patrick Eckland

- CPG expertise
- 7 years experience in financial planning, analysis, and accounting
- B.S. in Finance, M.S. in Data Science candidate, MBA candidate.

Satvik Yagnamurthy

- Healthcare expertise
- 3 years experience in growth strategy, M&A, and program management
- B.S. in Industrial Engineering, M.S. in Data Science candidate

Yemi Adetutu

- Statistics expertise
- 10 years experience in Network Optimization, , and Business Development
- B.S. in Statistics & Mathematics, M.S. in Data Science candidate

Yinwei Wang

- Medtech expertise
- 4 years experience in upstream marketing, 3 years downstream marketing, 1 years in venture capital and 3 years in CPG
- B.A. in Human Resources, MBA, M.S. in Data Science candidate

Jamia Russell

- Research expertise
- 3 years experience in growth strategy, M&A, and program management
- B.A. in Criminology, Psychology, Chinese, M.S. in Data Science candidate

Company Overview

Logistics

- Location: Established in 2019, Gold Coast, Chicago
- Size: 15,000 square feet, modern equipment
- Hours: Open 5:00 AM – 10:00 PM daily
- Memberships: Monthly, annual, and family options

Strengths

- Prime Location: High-traffic, affluent area
- Modern Facilities: Advanced equipment and spacious layout
- Variety: Classes and training for all fitness levels
- Community: Regular fitness events and challenges

Financial Model

- Revenue: Membership fees, personal training, classes
- Pricing: Tiered plans—basic, premium, family
- Add-ons: Extra services like training and nutrition
- Costs: Rent, staff salaries, equipment upkeep

Areas for Improvement

- Lack of Digitization: Fitness Center has an outdated mobile application and website
- Negative Data Experience: Users are unable to track logistical and fitness metrics to enhance engagement

Assessment Approach: Zero Trust Framework

1 People/Identity

User access management prioritizing verification and authentication methods including least privilege access policy

2 Devices

Ensure device compliance with security controls

3 Applications

Mitigate application specific threats through integrated protections

4 Data

Inventory, categorize, and label data mechanisms to prevent data exfiltration

5 Network

Augment network to defend segmentation, encryption, and host isolation

6 Infrastructure

Monitor network, data, and API use and access vulnerabilities and audit to compliance standards

Maturity Model

Traditional

❑ On-premises identity providers with limited visibility into identity risks;

❑ Device are normally through internal IT system such as Group Policy Object and needs to be on network to access data

❑ Applications can only be accessed through physical network or VPNs; No cloud apps

❑ Network security is minimal and minimal threats protection;

❑ Data classification and protection are inconsistent; data access is more governed by perimeter control not data sensitivity

❑ Infrastructure permission and access needs to be manually managed

Advanced

❑ Hybrid identity systems in place–conditional access policies for access to data, applications and networks

❑ Devices are registered with cloud identity providers and access only granted to cloud managed & compliant devices

❑ On-premises apps are internet-facing and cloud apps are using SSO

❑ Network cloud threat protection is in place; Network has some level of micro-segmentation

❑ Data is well classified and labeled via regex/keyword methods; access decisions encrypted

❑ Infrastructure management are more automatic, with monitoring system and anomalies detection; every workloads is assigned app identity; human access to resources requires just-in-time (only when needed)

Optimal

❑ Cloud identity with real-time analytics to determine risk and deliver ongoing protection; passwordless authentication is implemented

❑ Device risk is minimized by access control; endpoint threat detection is used to monitor device risk.

❑ Apps are using least privilege access with continuous verification; dynamic control is in place with in-session monitoring

❑ Network is fully segmented with micro-perimeters and encryption and all traffic is encrypted

❑ Data access decisions are fully governed by cloud security policy and data sharing is secured with encryption and tracking

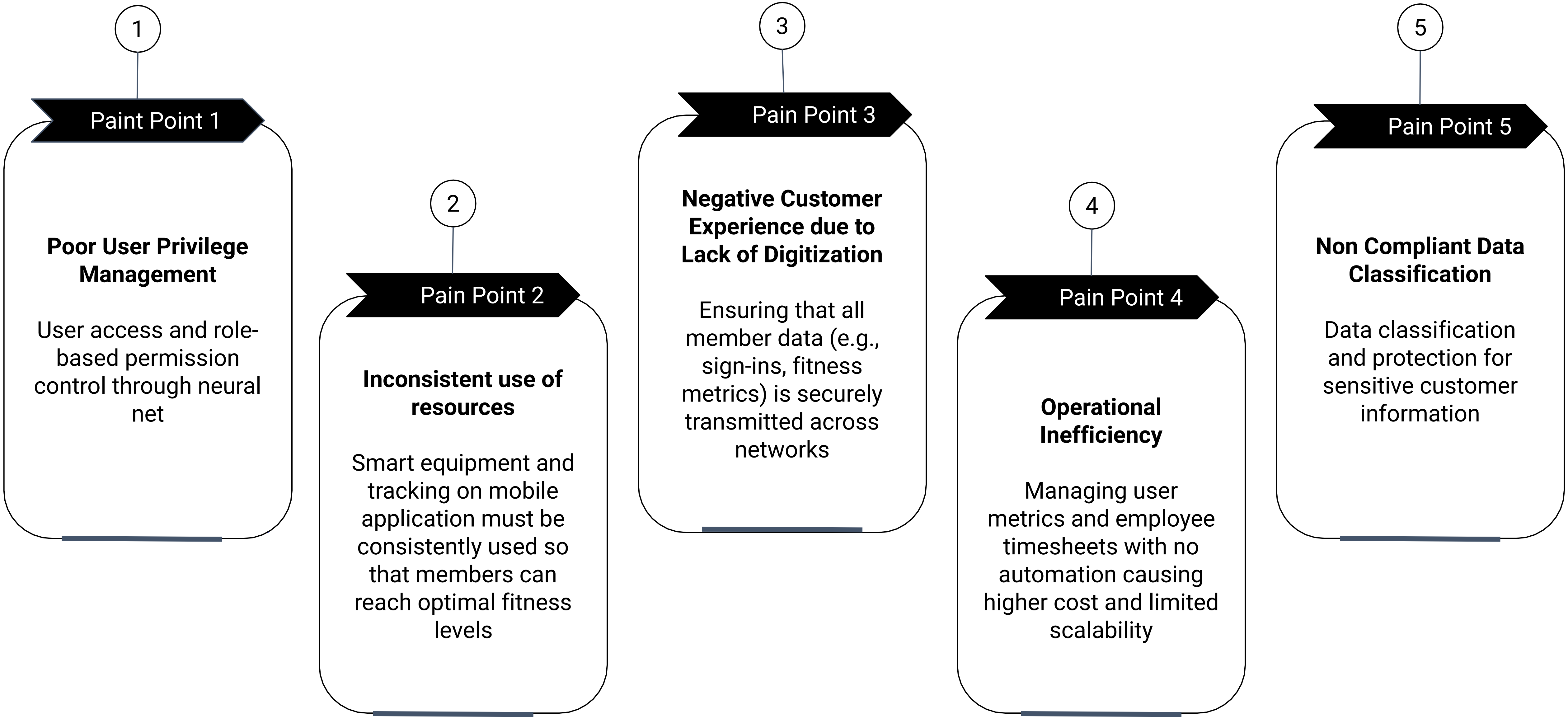
❑ Infrastructure is completely automatic and monitored for abnormal behavior with granular visibility and access control; unauthorized deployments are blocked and alert is triggered users and resources access is segmented for each workload

Zero Trust Maturity Model–Download Center–Microsoft:

Current State Assessment

Capabilities	Business Needs	Current/Target Maturity
People/Identity	User specific permissions (managers, employees, members, class instructors) controlling sign-in and data access	Traditional -> Advanced
Devices	Secure integration with Management System and connected devices (fitness equipments, member devices and applications compatibility)	Traditional -> Advanced
Applications	Employee level provisioning based on smart approvals to limit and grant access to employees, members, and instructors	Traditional -> Advanced
Data	User-based access, data encryption, and activity logging to protect and report personal information and fitness metric	Traditional -> Advanced
Network	Data security and system monitoring to track unusual activity, unauthorized access to internal tools	Traditional -> Advanced
Infrastructure	Necessity for architectural components that will monitor network, data, API use, and access vulnerabilities and audit to compliance standards	Traditional -> Advanced

Pain Points



1

Paint Point 1

Poor User Privilege Management

User access and role-based permission control through neural net

2

Pain Point 2

Inconsistent use of resources

Smart equipment and tracking on mobile application must be consistently used so that members can reach optimal fitness levels

3

Pain Point 3

Negative Customer Experience due to Lack of Digitization

Ensuring that all member data (e.g., sign-ins, fitness metrics) is securely transmitted across networks

4

Pain Point 4

Operational Inefficiency

Managing user metrics and employee timesheets with no automation causing higher cost and limited scalability

5

Pain Point 5

Non Compliant Data Classification

Data classification and protection for sensitive customer information

Pain Point 1: Poor User Privilege Management

People/Identity **Network**

Assessment

Michigan Ave. Fitness Center app current role designations lack distinct permissions reflective of user role - manager, standard employee, member category, and fitness class instructor profiles

Recommendation

It is recommended that Michigan Ave. Fitness Center administer data access and modification controls based on user role and activity status through MFA, and granular based permissions

Pain Point 2: Member willingness to utilize resources

People/Identity **Devices** **Applications** **Data**

Assessment

Members are not currently using their mobile device applications on a consistent basis. This includes syncing to the gym’s smart equipment, tracking/logging activities, and answering brief surveys on their experiences. As a result, the gym does not have accurate data to enhance member experience and advance fitness levels.

Recommendation

Michigan Ave. Fitness center must ensure staff is sufficiently trained to train and assist members with properly using the mobile app. We also recommend that members are required to watch a brief training video on how to navigate the mobile app upon joining the gym. This video will emphasis the importance of using the app for meeting their fitness goals. It will also provide assurance that their data and privacy is protected.

Pain Point 3: Negative customer experience due to Lack of Digitization

Data **Network**

Assessment

According to a 2021 publication by the International Journal of Environmental Research and Public Health, it is shown that the use of the fitness app, as a single download or use element, improves habits, satisfaction or the intention to stay in the fitness center. Michigan Avenue Fitness Center’s app does not have the capability for members to track fitness metrics in a protected manner.

Recommendation

Implement secure data transmission - ensuring that all member data is transmitted across networks, both within the gym and through the mobile app, while preventing unauthorized interception or access during transmission. This requires strong encryption and network security protocols.

Pain Point 4: Operational Inefficiencies

People/Identity **Devices** **Applications** **Data**

Assessment

Unnecessary access to systems due to role-based updates has increased security risks. In the case of IoT, our manual device tracking and outdated employee check-in system increase downtime and create the possibility of human error. Additionally, our point-of-sale (POS) systems are not fully integrated with the Gym Management System, leading to manual processes and duplicate work

.

Recommendation

By utilizing automated data collection, reporting systems, and an identity management system, we can ensure that permissions are updated in real-time and synchronized across all systems, reducing the need for manual tracking and minimizing downtime. With our integrated applications, we can schedule in real-time, ultimately optimizing our operational workflow for years to come.

Pain Point 5: Non Compliant Data Classification

Data

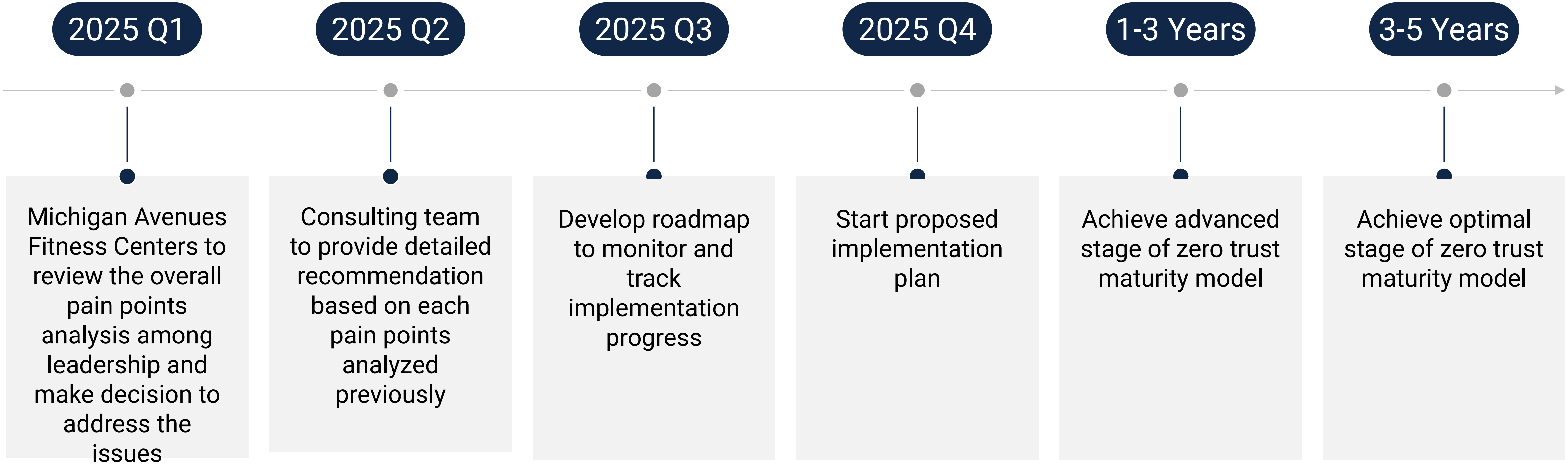
Assessment

No formal process for classifying data based on its sensitivity and importance (e.g. payment information, fitness profile), leading to insufficient protection on sensitive data

Recommendation

We recommend Michigan Avenue Fitness Center to ensure compliance with data privacy regulations such as GDPR or HIPPA, to leverage automated data classification tools to better categorize data based on the sensitivity and importance, and to establish encryption system for all sensitive data to prevent unauthorized access and breaches

Next Steps - Implementation Plan



2025 Q1

Michigan Avenues Fitness Centers to review the overall pain points analysis among leadership and make decision to address the issues

2025 Q2

Consulting team to provide detailed recommendation based on each pain points analyzed previously

2025 Q3

Develop roadmap to monitor and track implementation progress

2025 Q4

Start proposed implementation plan

1-3 Years

Achieve advanced stage of zero trust maturity model

3-5 Years

Achieve optimal stage of zero trust maturity model

Thank You!

Michigan Avenue Fitness Center

Reference

Pagliaro, Maria, Chiara Di Martino, Federica Currà, and Martina Mangiacapra. 2021. “Gym Facilities in the Post-COVID Era: A New Challenge for Safety and Health.” International Journal of Environmental Research and Public Health 18 (19): 10393. https://doi.org/10.3390/ijerph181910393.

“Zero Trust Maturity Model–Download.microsoft.com”, Microsoft, 2022: https://download.microsoft.com/download/f/9/2/f92129bc-0d6e-4b8e-a47b-288432bae68e/Zero_Trust_Vision_Paper_Final%2010.28.pdf