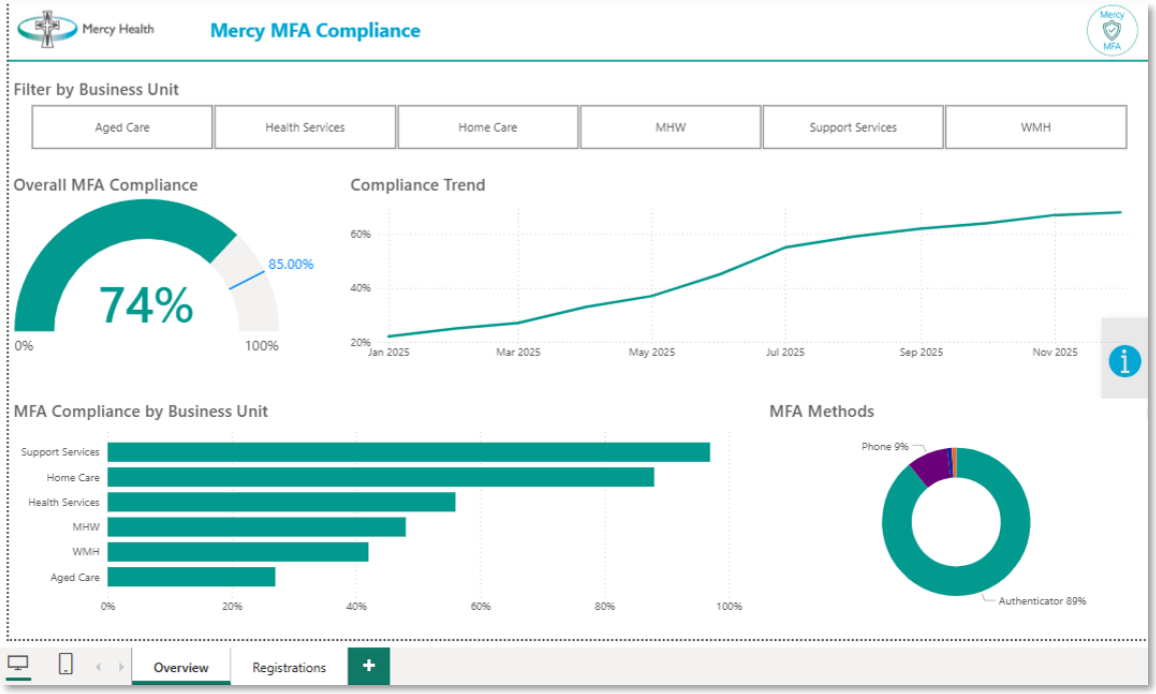
WARREN SPIER

CASE STUDY

Driving Identity Security through Automated MFA Governance Analytics

Mercy Health

Microsoft



My role

In the context of the broader Digital Transformation Program I was leading, we faced rigorous cybersecurity maturity measures set by the Department of Health. To meet these, I engineered a technical approach to synthesise security telemetry and HR metadata, empowering leadership with the granular insights needed to dismantle a fragmented MFA ecosystem and shift the organisation from a vulnerable state to a best-practice trajectory.

Background

Mercy faced a significant security maturity gap. The organisation operated within a fragmented MFA ecosystem characterised by low enrolment rates and a lack of centralised visibility.

- **The Risk:** Minimal MFA adoption created an expansive attack surface, leaving sensitive health and corporate data exposed to credential-based attacks.
- **The Cultural Barrier:** There was a prevailing lack of urgency regarding identity security. Without granular data, it was impossible to hold business units accountable or demonstrate the specific areas of risk.

The Solution

Data Engineering:

- Automated Identity Telemetry: Developed a custom ingestion pipeline using the Microsoft Graph API to retrieve live authentication method registrations (Authenticator app, Phone, FIDO2, etc.) from Microsoft Entra.
- HCM Synthesis: Performed a complex join with Workday HCM data. This allowed for multi-dimensional modelling across Business Unit, Location, and Employment Type.

Skills

- Data Visualisation
- Data Analysis
- API Integration
- Cybersecurity
- Change Management

Tools

- Power BI
- Microsoft Graph API
- Workday
- Power Query
- DAX

- Data Transformation: Using Power BI's M-engine and DAX, I resolved data fragmentation issues, aligning disparate identity markers between the security and HR ecosystems to create a single source of truth.

Data Analysis:

- Drill-Down Logic: Created a hierarchical model allowing stakeholders to move from a 30,000-foot organisational view down to specific departments.
- Trend Forecasting: Utilised time-series analysis to visualise the "MFA Compliance Trend," identifying that while the overall rate was 68%, specific units like "Aged Care" were lagging significantly at 27%, requiring targeted intervention.
- By applying linear regression to the compliance trend, I was able to forecast that Mercy would hit its 80% "Best Practice" target by February 2026, providing the executive team with a clear, data-backed roadmap.

Visualisation and UX Design:

- Strategic Layout: Designed the dashboard using a "Summary-to-Detail" approach. High-level KPIs (Actual vs. Target) are positioned at the top, followed by a Business Unit Compliance bar chart to drive internal accountability.
- Method Composition: Integrated a distribution analysis of MFA methods (Authenticator vs. Phone vs. Passkey) to encourage the shift toward more secure, "Phishing-Resistant" methods.

Results

- **Risk Reduction:** Successfully transitioned Mercy from a high-exposure state (22% compliance) to a robust 68% and climbing, significantly hardening the identity perimeter.
- **Cultural Shift:** The automated, transparent reporting created a "gamification" effect among Business Unit leaders. By seeing their specific compliance scores compared to peers (e.g., Support Services at 97% vs others), a culture of accountability and security awareness was established.
- **Operational Excellence:** Automated a previously manual process, enabling the Security team to focus on ongoing change management and user support rather than data collection.