# Bayside Health Partners

*Confidential briefing for the incoming security leadership team. Fictitious company; any resemblance to a real organization is accidental.*

**Who they are.** Regional nonprofit health system headquartered in Tampa, FL. Four hospitals, eleven outpatient clinics. 7,500 staff. 1.6 million active patient records. $950M annual revenue. Regulated under HIPAA; accepts card payments (PCI DSS) at all facilities.

**Technology.** Two years into a three-year migration from an on-premise EHR to a cloud-hosted platform; both environments run in parallel today. Roughly 2,400 connected medical devices, many on operating systems the vendor no longer supports. Microsoft 365 for productivity. A single regional billing processor handles all claims.

**Security posture.**

- Phishing-resistant MFA enforced on every account, including contractors, verified quarterly. (The one thing the last CISO finished.)
- Security team of nine. An MSSP forwards alerts overnight; nobody in-house watches screens between 11 PM and 7 AM.
- Critical patches reach the general estate in about three weeks. Medical devices patch on the vendor's schedule or never.
- Immutable backups deployed for the cloud EHR only; the legacy EHR backs up to the same network segment it runs on.

**History.**

- Ten months ago: ransomware encrypted two hospitals' imaging systems. Bayside paid $400K to restore operations. Total event cost near $2.8M.
- Last year: a business email compromise moved $340K to a fraudulent account; $190K was recovered.

**Open risk register (extract).**

1. Legacy-EHR backups share a network segment with production (open 14 months).
2. Billing-processor contract carries no security requirements and no breach-notification clause (open 9 months).

**From the CFO.** The audit committee's materiality trigger is $2.5M. The board meets in 45 minutes.

**Odd tables, insurance:** accept the renewal or not.

- $10M tower with a $250K retention.
- Premium today: $180K a year. Renewal quote: $252K a year, up 40%.

**Even tables, the $1.2M:** fund the security team's request, $1.2M a year, or not. MFA is already in place.

- Segmentation of the medical-device network: $600K a year.
- Patching discipline, devices included: $400K a year.
- Immutable backups for the legacy EHR: $125K a year.
- Incident-response retainer: $75K a year.