Meeting Notes / MoM: Cyber Underwriting & Capital Allocation Strategy

Meeting Details

Client: NorthStar Mutual Insurance
Topic: FY27 cyber portfolio risk review, underwriting directives, capacity allocation, and reinsurance alignment
Date: 18 June 2026
Meeting type: Consulting team and client executive working session
Objective: Convert portfolio performance, sector risk, and reinsurer feedback into FY27 board-ready underwriting actions.

Attendees

NorthStar Mutual Insurance

- Karen Liu, Chief Underwriting Officer
- Daniel Ortiz, Head of Cyber Portfolio
- Meera Shah, Chief Risk Officer
- Thomas Reed, Reinsurance Lead
- Priya Menon, Claims Analytics Lead

Apex Strategy Consulting

- James Carter, Partner
- Riya Malhotra, Engagement Manager
- Alex Chen, Cyber Risk Expert
- Nora Williams, Associate

Context

NorthStar's cyber book grew from **$870M in FY25 GWP** to **$1.08B in FY26 GWP**, but profitability weakened. The overall cyber loss ratio increased from **58% to 71%**, driven mainly by ransomware frequency, business interruption severity, public-sector control gaps, healthcare legacy systems, and vendor outage aggregation in logistics.

The executive team wants an FY27 board recommendation that protects profitability without creating the impression of a broad retreat from cyber insurance.

Portfolio Discussion

Management target is to reduce the FY27 loss ratio below **62%**.

Total book shrinkage should remain below **5%** if possible.

Growth should shift from volume-led underwriting to control-led capital allocation.

Reinsurers are asking for stronger evidence of MFA, offline backups, endpoint controls, vendor dependency mapping, and aggregation discipline.

The consulting team recommended framing the strategy as **capital reallocation**, not simply underwriting tightening.

Segment Review

Municipalities & Public Sector

FY26 capacity: $160M
Proposed FY27 capacity: $120M
Loss ratio status: High loss
Reinsurance support: Under review

Claims frequency is elevated due to ransomware attacks on city agencies, public utilities, and county systems. Budget constraints are slowing remediation. Several insureds lack consistent MFA coverage across departments, while offline backup testing is inconsistent and often not documented.

Renewal should require MFA, validated offline backups, endpoint detection, and a named incident commander. Accounts with unsupported operating systems in critical departments should be declined or moved to sharply reduced limits.

Tier-1 Financial Institutions

FY26 capacity: $320M
Proposed FY27 capacity: $350M
Loss ratio status: Stable
Reinsurance support: Strong

Banks and large financial institutions show stronger cyber hygiene than other sectors. Continuous monitoring, independent penetration testing, and mature incident response processes are common. Reinsurers remain comfortable with this segment.

Selective premium credits can be offered where real-time compliance monitoring is in place. Capacity should be maintained or increased, but only for institutions with strong control evidence.

Healthcare & Medical Systems

FY26 capacity: $210M
Proposed FY27 capacity: $180M
Loss ratio status: Elevated
Reinsurance support: Strong but selective

Legacy medical devices are a major entry point for attackers. Network segmentation is uneven across hospital systems. Business interruption severity is high because downtime affects patient operations.

Deductibles should increase by approximately **20%** for institutions without segmented networks. Disaster recovery testing should be mandatory within the last 12 months.

Supply Chain & Logistics Providers

FY26 capacity: $130M
Proposed FY27 capacity: $95M
Loss ratio status: Elevated
Reinsurance support: Weak

Vendor downtime and software-provider concentration are creating aggregation risk. Class-action exposure is increasing after extended service outages.

New business should face tighter aggregate limits. Third-party vendor risk audits should be required before writing large limits. Policy language should include clearer sublimits or exclusions for prolonged vendor downtime where visibility is weak.

Mid-Market Professional Services

FY26 capacity: $140M
Proposed FY27 capacity: $145M
Loss ratio status: Stable
Reinsurance support: Moderate

This segment remains acceptable if minimum controls are enforced. Renewal conditions should include MFA, privileged access controls, endpoint detection, and employee phishing training.

Pricing discipline should remain firm, but capacity does not need to be reduced materially.

Retail & E-Commerce

FY26 capacity: $115M
Proposed FY27 capacity: $105M
Loss ratio status: Elevated
Reinsurance support: Moderate

Payment data exposure and seasonal transaction peaks increase breach severity. Controls vary meaningfully by account size.

Larger accounts should provide evidence of PCI compliance, tokenization, incident response testing, and payment processor dependency mapping.

Decisions Taken

- Reduce public-sector capacity from **$160M to $120M**.
- Increase Tier-1 financial institution capacity from **$320M to $350M**.
- Reduce healthcare capacity from **$210M to $180M**.
- Reduce supply-chain and logistics capacity from **$130M to $95M**.
- Hold mid-market professional services broadly stable at **$145M**.
- Reduce retail and e-commerce capacity modestly to **$105M**.
- Link underwriting appetite directly to control evidence and reinsurance support.
- Present the board message as disciplined capital allocation rather than broad market withdrawal.

Reinsurance Feedback

Reinsurers are comfortable backing financial institutions.

Healthcare remains insurable where network segmentation and disaster recovery evidence are strong.

Public-sector support will depend on proof of remediation.

Logistics is the most difficult segment because vendor concentration creates hidden aggregation.

The reinsurance lead noted that capacity is still available, but not for undifferentiated cyber risk.

The treaty renewal narrative should emphasize segmentation, control enforcement, and improved portfolio visibility.

Board-Level Message

FY27 cyber strategy should shift from growth-led underwriting to risk-adjusted capital allocation. NorthStar can protect premium volume while improving profitability by moving capacity away from high-frequency ransomware segments and toward sectors with verifiable controls, stronger reinsurer support, and lower aggregation risk.