ICSC 2026 Round 3 Scenario



Note: REGARDLESS of what happened in Round 2, THIS is the Round 3 scenario that covers what really happened in Round 2. You are to assume this information below when planning for Round 3.

Your meeting with Matt Olinger went well! You learned more about FBMC's issues and confirmed that they want a solution quickly to their cybersecurity problems. Matt confirmed the Microsoft security tools and that they only have 4 people responsible for security operations, but they are considering hiring 6 more at a cost of $720,000. Matt said FBMC has around 11,000 endpoints.

Matt confirmed that FBMC had multiple critical incidents at once. Plus, the 180 alerts they get a day stretches their security team. All four security people stop their other work and piece together what happens across several tools. Matt said the improvements to their defenses keep getting pushed back, namely threat hunting, improving detection coverage, and identifying gaps. Matt is worried that these delays might let an incident slip through. No client or benefits-related information has been compromised—yet. Hiring six more people would help, but that could take months and there would still be the same manual processes in place. And the existing team might quit because of burnout.

Matt confirmed that FMBC does not have a clear view of every device and system. Info from different tools does not always match. During the recent incidents, it was difficult to confirm which systems were involved and whether they had the protection expected. Some devices are on IT's inventory but don't have security software. Other devices aren't sending data that security needs to respond to threats. They can check these gaps manually, but things keep changing. A new system can be added, or a security tool can stop reporting, making the last review out of date. FBMC needs a way to spot missing coverage and send confirmed gaps to the team so they can fix them—before an incident happens.

Finally, Colin explained that the quality of an investigation can depend too much on which person handles it. Their analysts are capable, but the steps taken and the evidence captured are not consistent. Handing an incident to another analyst means more dwell time. Leadership also has difficulty understanding what was found and why an action was recommended. Matt wants to see the evidence and reasoning behind a recommendation, not just a verdict. FBMC's goal is to have repeatable investigations, understandable recommendations, and a clearer record of what the team did.

At the end of the meeting, Matt said that Rick (Rachel) Farris would make the final call for FBMC. (https://www.linkedin.com/in/rick-farris-a9aa6214/). You asked for an intro to Rick (Rachel) and got a fast response. You have a 20-minute meeting with Rick (Rachel) on Friday afternoon. Good luck!