



CASE STUDY: **COMMUNITY FIRST BANK OF INDIANA**

STRENGTHENING
CYBER RESILIENCE
THROUGH
FRACTIONAL CISO
LEADERSHIP

BANK SNAPSHOT

- **Founded:** 2003
- **Assets:** ~\$900M
- **Headquarters:** Indiana
- **Footprint:** Central Indiana
- **Engagement:** Fractional CISO Leadership

As Community First Bank of Indiana (CFB) grew toward the \$1 billion asset mark, leadership recognized that cybersecurity had become an enterprise risk requiring executive and board-level oversight. At the same time, the bank no longer had a dedicated information security leader, creating a gap in accountability as cyber threats increased across the industry. With peer institutions experiencing visible incidents and regulators raising expectations around governance and documentation, leadership understood that a single successful attack could disrupt operations, erode customer trust, and damage the bank's reputation at a pivotal moment in its growth.

A Growing Concern:

“What if we are next?”

As CFB approached one billion dollars in assets, leaders began asking urgent questions about accountability and preparedness. Those concerns intensified when targeted phishing attempts nearly compromised executive credentials, demonstrating how quickly a single mistake could create a pathway into critical systems.

Shortly thereafter, a third-party vendor supporting the bank’s ATM network experienced a ransomware attack. While the bank itself was not the source of the breach, the incident underscored how quickly operational and reputational risk could escalate without strong leadership and response capabilities in place.

Leadership identified three immediate risks that required action:

- A cybersecurity leadership vacancy with no clear dedicated team
- Increasing regulatory scrutiny and higher expectations for governance
- Near-miss incidents involving executive credentials that signaled exposure

The bank needed experienced cybersecurity leadership and a mature, scalable program.

Engaging Fractional CISO Leadership

CFB partnered with Hartman Executive Advisors to implement a comprehensive cybersecurity program led by a fractional CISO. This approach allowed the bank to put seasoned leadership in place immediately while gaining access to a broader team of specialists supporting governance, monitoring, incident response, and regulatory alignment.

Hartman served as the bank's accountable CISO, working directly with executive leadership, the board, and internal IT staff. Rather than operating as a traditional advisor, the Hartman CISO and supporting team assumed day-to-day ownership of the cybersecurity program, allowing executives to stay informed and confident without having to manage the details themselves.

Hartman began with a full assessment of the bank's technology environment, risk posture, and compliance requirements. A formal governance structure was established that clearly separated operational IT responsibilities from independent information security oversight, aligned the program with examiner expectations, and clarified accountability across the organization.

A cross-functional security steering committee was created to manage cybersecurity as an enterprise priority, providing leadership with consistent visibility into risk, program maturity, and progress.

Detecting and Containing Real Threats

With governance in place, Hartman implemented managed detection and response through a dedicated security operations center.

When sophisticated phishing campaigns targeted executive-level users, enhanced monitoring identified anomalous activity quickly. Access was terminated, credentials were reset, and potential lateral movement was prevented, strengthening leadership's confidence in the bank's security posture.

During Hartman's engagement, the ATM vendor ransomware incident tested the program in real time. Hartman guided the response by isolating systems, reviewing indicators of compromise, and managing stakeholder communications. The bank returned to normal operations without customer disruption.

“Hartman has done a lot more than just advise us on cybersecurity. They stepped into the CISO role and took ownership of the program, which has made a real difference for our team.”

Results That Restored Confidence

Through Hartman's fractional CISO leadership, CFB moved from uncertainty to a governed, well-controlled cybersecurity program. Outcomes included:

- A stronger regulatory position
- Reduced operational and reputational risk through effective detection and response
- Defined governance, clear ownership, and increased confidence at the executive and board level

“Hartman’s fractional CISO model gave our leadership and board the confidence that our cybersecurity program was being run with true independence and expertise. It’s given us peace of mind in a way we hadn’t experienced before.”

The fractional model delivered immediate access to seasoned expertise at a lower cost than a full-time executive, while allowing the program to scale alongside the bank's continued growth.

Conclusion

By partnering with Hartman Executive Advisors for fractional CISO leadership, Community First Bank of Indiana addressed a critical leadership gap, strengthened its cybersecurity posture, and built a governance structure that delivers clarity and confidence. The bank is now better prepared to protect its customers, its reputation, and its long-term franchise value as it continues to grow.