Community Bank Security Starter Kit

A practical starting point for community bank security.

Table of Contents

Introduction

Most community banks know they need better security. The question is where to start without blowing the budget or overwhelming your team.

This kit gives you a practical path forward: a scorecard to identify your gaps, quick wins that examiners actually care about, and clear guidance on when to bring in help.

No fluff. No 50-page policies. Just the controls that matter for community banks and credit unions.

A note from Lora

I've worked in cybersecurity for over a decade, including CISO roles at banks and FinTechs dealing with everything from wire fraud to regulatory exams. I've seen what works and what doesn't.

Here's what I know: you don't need to be a security expert to protect your bank. You need to focus on the right controls, have a plan for when things go wrong, and know when to call in help. That's what this kit is for. Use it, adapt it, and don't overthink it.

Quick Wins for Community Banks

5 Security Controls That Actually Matter

Most community banks don't need a complete security overhaul. You need to focus on the controls that protect customer data, satisfy examiners, and don't require a massive budget. These are the 5 controls that give you the most impact with the least pain:

1. Multi-Factor Authentication (MFA) Everywhere

Why it matters: Stops 99% of account takeover attacks. Examiners ask about it in every audit.

Quick win: Turn on MFA for all email accounts and any system that touches customer data. Start with admin accounts if you need to phase it in.

Cost: Usually free or already included in your Microsoft/Google subscription.

2. Automated Patch Management

Why it matters: Unpatched systems are the #1 way attackers get in. Ransomware loves outdated software.

Quick win: Set up automatic updates for workstations and servers. If you can't automate, create a monthly patch schedule and stick to it.

Cost: Minimal. Most patch management tools are included in endpoint protection you already pay for.

3. Email Security Beyond Basic Spam Filtering

Why it matters: Wire fraud and phishing are the biggest threats to community banks. Your customers and employees are targets.

Quick win: Add email authentication (SPF, DKIM, DMARC) and advanced threat protection. Block executable attachments.

Cost: $3-5 per user per month for advanced protection.

4. Centralized Logging

Why it matters: You can't investigate what you can't see. Examiners want proof you can detect incidents.

Quick win: Set up logging for failed login attempts, admin changes, and file access. Keep logs for at least 90 days.

Cost: Can start with free tools (Windows Event Forwarding) or basic SIEM at $500-2000/month.

5. Incident Response Plan That Actually Works

Why it matters: Not having a plan when something goes wrong costs you days of recovery time and thousands in emergency consulting fees.

Quick win: Document who does what when systems go down. Include your vendors' emergency contact info. Test it once a year.

Cost: Free if you write it yourself. $5-10K if you hire someone to build it for you.

What's Next?

If you can knock out these 5 controls, you're ahead of most community banks. If you're stuck on any of them or want someone to validate your current setup, that's what fractional CISO support is for.

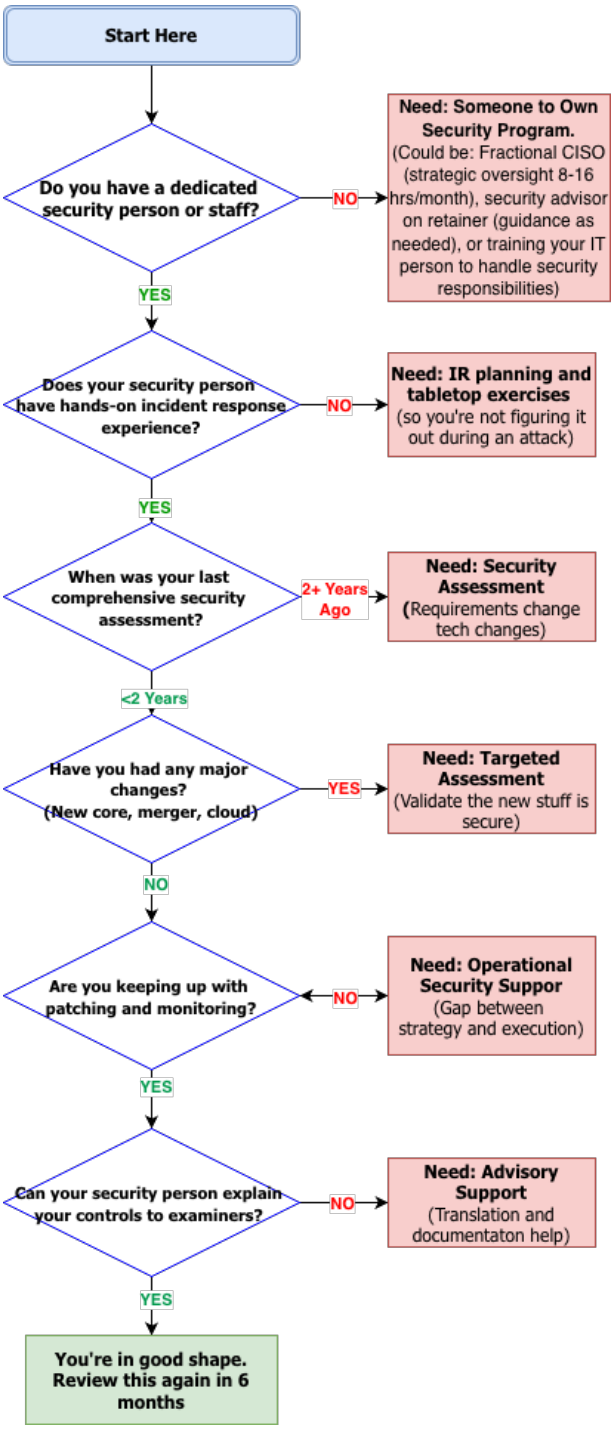
Want the full scorecard? Use the CIS Controls Scorecard included in this kit to see where you stand across all 18 CIS Critical Security Controls.

When to Call in Security Help

Most community banks have some security in place. The question isn't whether you need security, it's whether what you have is enough and whether you need outside help to fill the gaps.

Use this decision tree to figure out where you stand and what kind of support makes sense for your bank.

Decision Tree



CIS 18 Controls Scorecard

This scorecard helps you assess your current security posture against the 18 CIS Critical Security Controls. It's the same framework examiners reference, which means filling this out gives you a head start on your next audit.

What you get

An Excel template that walks through each control and lets you score your implementation on a 0-5 scale:

- **0** = Not doing this. Period.
- **1** = Reactive/Ad hoc. Someone remembers how to handle it eventually.
- **2** = Inconsistent. Maybe there's a process somewhere, but it depends who's handling it.
- **3** = Repeatable. Documented process that works the same way each time.
- **4** = Solid. Process is documented, followed, and makes sense. You could hand this to a peer CISO without embarrassment.
- **5** = Optimized. Efficient, automated where it matters, continuously improved.

How to use it

1. **Be honest about your scores.** This is for you, not examiners. If you're inflating scores, you're only hurting yourself.
2. **Focus on the 0s and 1s first.** These are your biggest risks. Use the Quick Wins section to prioritize what to tackle.
3. **Don't expect all 5s.** Most community banks will have a mix of 2s, 3s, and 4s. That's normal. Perfect is the enemy of good enough.
4. **Review it quarterly.** Your security posture changes as you implement new controls or add new systems. Update the scorecard every 3-6 months.

Download the scorecard:

https://downloads.vaughncybergroup.com/CIS_Controls_Scorecard_v1.xlsx

Need help interpreting your results?

That's what a fractional CISO is for. We can review your scorecard, prioritize your gaps, and build a roadmap that makes sense for your budget.