

Guarding the Gates

Cybersecurity as a Ministry of Stewardship · A Leader's Companion

Dr. Laura A. Jones · October 26, 2026

"Let not the gates of Jerusalem be opened until the sun be hot ... and appoint watches of the inhabitants of Jerusalem, every one in his watch, and every one to be over against his house."

— Nehemiah 7:3 (KJV)

The Gate Changed. The Stewardship Didn't.

Church leaders have always guarded what matters most: God's people. Today, much of what you protect lives online: member records, giving, children's registrations, counseling notes, payroll, and the email account with your pastor's name on it. Most cyber threats don't break in; they persuade someone to open the door. The good news is that the habits that protect your church are leadership habits, not technical ones.

Guard the People Gate

Behind every record is a person. These are the people who trust your church with their information:

				
The Congregation	The Family	The Child	The Employee	The Guest Minister
Online giving and prayer requests	Counseling and care records	Youth registrations and check-in	Payroll and banking details	Personal and travel details

Five Questions for Your Leadership Team

Take these back to your leadership team. Afterward, record your first answers and who will own the follow-up.

#	Question · Principle	Our first answer · Owner
1	What information has God entrusted to our care? STEWARDSHIP	
2	Who has access to it, and why? ACCOUNTABILITY	
3	What aspects of our church culture enable vulnerability? SHARED RESPONSIBILITY	
4	If our systems were unavailable this Sunday, how would our ministry continue? RESILIENCE	
5	How would we know if someone were impersonating one of our leaders? VIGILANCE	

Guard the Money and Data Gate

Attackers want two things: money and data. Business email compromise needs only a trusted name and a willing hand: a message that seems to come from the pastor, or a vendor whose “bank details have changed.” Member records, donor details, children’s registrations, and passwords are just as valuable: they can be sold, misused, or published. Four habits stop most of it:

- ☐ **Call back on a known number** before acting on any unexpected request for money, gift cards, changed payment details, or sensitive information. Use the number you already have, never the one in the message.
- ☐ **Require two approvers** for wires and electronic transfers.
- ☐ **Keep sensitive information in church systems.** Share it through approved, protected tools, not personal email or text, and remove access promptly when someone’s role changes.
- ☐ **Know your vendors** before trusting them with money or data. Sort them as normal, high, or critical risk, and focus your attention there.

Pause and verify when a request is urgent, secret, about money or data, or from an unfamiliar channel. “Believe not every spirit, but try the spirits” (1 John 4:1). “...for we are not ignorant of his devices” (2 Corinthians 2:11).

Ask your team: *How do we verify a request to change where money goes, and who can see our most sensitive records?*

Your First Three Steps

☐ THIS WEEK

Ask the five questions with your leadership team, and listen to the answers.

☐ OVER THE NEXT MONTH

Name an owner for each digital gate: giving, church management software, email, website, and livestream.

☐ THIS QUARTER

Rehearse how ministry continues if systems go down on a Sunday. Thirty minutes around a table is enough to start.

“For as the body without the spirit is dead, so faith without works is dead also.” — James 2:26 (KJV)

Notes

Going Deeper

The practices here grow out of the Biblically Framed Cybersecurity (BFCy) model; see BFCy at a Glance for the framework behind them. The question that was hardest to answer is often the best place to begin.

Let’s continue the conversation: DrJones@STEMulateMinds.com

