MissionDefend
Cybersecurity for churches & nonprofits

Grace Chapel (example)
120 members · 6 staff · 2 volunteers
Assessment completed 12 March 2026
Prepared for the board and leadership team

Your Cybersecurity Baseline

This report shows where your organization stands today, the risks that matter most right now, and exactly what to do about them over the next 30 days. It is written to be read by people who are not cybersecurity professionals.

LEVEL 2 — DEVELOPING

You have real protections in place. The gaps are in the places that matter most.

Your email security is genuinely good, largely because Microsoft 365 does a lot for you by default. But if someone locked up your files tomorrow, you could not confidently restore them — and no one has written down who to call. Those two gaps drive most of your score.

Level 1 Initial	**Level 2 Developing**	Level 3 Protected	Level 4 Managed	Level 5 Mature

Where you stand, category by category

Categories are weighted by how much each one actually reduces risk for an organization your size — not treated as equal. The weighted contributions add up to your score of 42.

CATEGORY	SCORE	RATING	WEIGHT	CONTRIBUTES
Identity & Access		**40%**	20%	8.00
Backup & Recovery		**30%**	18%	5.40
Email Security		**75%**	15%	11.25

CATEGORY	SCORE	RATING	WEIGHT	CONTRIBUTES
Endpoint Security		**65%**	12%	7.80
Security Awareness		**25%**	12%	3.00
Incident Response		**10%**	10%	1.00
Network Security		**60%**	8%	4.80
Policies & Governance		**15%**	5%	0.75
Overall		**42**	**100%**	**42.00**

THREE ANSWERS WERE "DON'T KNOW"

Nobody could say whether backups are tested, whether old volunteer accounts were ever closed, or who has administrator access to your giving platform. That is not a failing — it is the most useful thing this assessment found. "Don't know" almost always means no one owns that area, and unowned areas are where problems grow quietly. Each one becomes an action below.

Your top 5 risks right now

Ranked by how much damage each could cause and how likely it is — not by how hard they are to fix.

1. Your backups have never been tested CRITICAL

Files are copying to a cloud drive, but no one has ever tried restoring them. An untested backup is a hope, not a plan — and the most common discovery during a ransomware incident is that the backup was silently failing for months, or that it was connected in a way that let the attacker encrypt it too.

If this goes wrong: member records, giving history and years of sermon and ministry files become unrecoverable. Recovery costs move from hours to months.

2. Two administrator accounts have no multi-factor authentication CRITICAL

Most of your staff have MFA turned on, which is genuinely good. But two accounts with administrator rights do not — and those are exactly the accounts an attacker wants. A stolen password on a normal account is a problem; a stolen password on an admin account is access to everything.

If this goes wrong: an attacker reads and sends mail as your pastor, changes payroll or giving details, and can lock you out of your own systems.

3. There is no written incident response plan HIGH

If a compromise happened on a Sunday morning, no one knows who to call first, who can authorize shutting something down, or who tells the congregation. Decisions get made under pressure by whoever happens to be nearby — which is how small incidents become large ones.

If this goes wrong: hours lost to confusion during the window when fast action matters most, plus a real chance of missing a legal notification deadline.

4. Former staff and volunteers may still have access HIGH

There is no checklist for removing access when someone leaves, and nobody could confirm whether accounts from past volunteers were ever closed. In most organizations this size, at least a few are still open — often with access to donor or member information.

If this goes wrong: data leaves with people who no longer serve, and a dormant unused account is one of the easiest ways in.

5. No one has been trained to recognize phishing MEDIUM

The most common attack on churches is not technical at all. It is a message that appears to come from the pastor asking a volunteer to buy gift cards, or a fake invoice sent to your bookkeeper. Your filters catch many of these; the ones that get through are stopped only by a person who recognizes them.

If this goes wrong: a well-meaning volunteer moves money in good faith, and it is rarely recoverable.

Your first 30 days

Sequenced so the highest-impact work happens first. Nothing here requires buying software, and most of it is free.

Week 1 — Close the two critical gaps

About 3 hours total

Turn on MFA for the two administrator accounts

Addresses risk 2 · **30–60 minutes** · Owner: IT volunteer · Free with Microsoft 365

Restore one file and one mailbox from backup, and write down that it worked

Addresses risk 1 · **1–2 hours** · Owner: IT volunteer · This is the single most valuable hour in this plan

List every account with administrator access and confirm each person still needs it

Addresses risks 2 and 4 · **45 minutes** · Owner: Church administrator

Week 2 — Close the doors nobody is watching

About 2 hours total

Disable accounts for anyone who has left in the past two years

Addresses risk 4 · **1 hour** · Owner: Church administrator

Confirm who has administrator access to your giving platform

Resolves a "Don't know" answer · **20 minutes** · Owner: Finance lead

Check that automatic updates are on for every staff computer

Strengthens endpoint security · **30 minutes** · Owner: IT volunteer

Week 3 — Write down what only lives in people's heads

About 2 hours total

Fill in the one-page incident response plan template

Addresses risk 3 · **45 minutes** · Owner: Executive pastor · Template provided

Adopt the offboarding checklist so access is removed the same week someone leaves

Prevents risk 4 from returning · **30 minutes** · Owner: Church administrator

Adopt a written password and acceptable-use policy

Addresses policies score · **30 minutes** · Owner: Executive pastor · Template provided

Week 4 — Bring people in, then re-measure

About 2 hours total

Run a 20-minute staff and volunteer session on recognizing fake requests for money

Addresses risk 5 · **30 minutes to prepare** · Owner: Executive pastor

Agree a verify-by-phone rule for any payment or bank detail change

Addresses risk 5 · **15 minutes** · Owner: Finance lead · Free, and stops the most common loss

Retake the assessment and compare

Confirms the work held · **20 minutes** · Owner: Church administrator

WHAT THIS PLAN IS WORTH

Completing these twelve items moves this organization from **42 to an estimated 71** — from Level 2 to Level 3, Protected. Total cost: about nine hours of someone's time and no new software.

What is already working

Worth saying plainly, because it is easy to read a report like this and conclude everything is broken. It isn't.

- ✓ Multi-factor authentication is on for most staff accounts
- ✓ Spam and phishing filtering is active and correctly configured

- ✓ Staff computers run supported, up-to-date operating systems
- ✓ The guest Wi-Fi is separated from the staff network
- ✓ Giving is handled by a reputable provider, so card data never touches your systems
- ✓ Antivirus is running and reporting on every staff device

How this score is calculated

Your answers map to security controls drawn from the **CIS Controls** and the **NIST Cybersecurity Framework**. You never have to read either one — that translation is our job.

Each category is scored from 0–100% based on the controls you have in place. Categories are then weighted by how much they reduce real-world risk for an organization of your size and type, and the weighted results are added together: `overall = Σ (category score × weight)`. Backups and identity carry the most weight because they prevent the incidents that actually shut small organizations down; written policies carry the least, because a policy nobody follows protects nothing.

A question answered **"Don't know"** is never scored as if you had said yes. It is counted as a gap in visibility and generates its own action, because not knowing is a finding in itself.