UMC INFORMATION TECHNOLOGY SUPPORT

CHURCH'S SURVIVAL GUIDE FOR A CYBERSECURITY JOURNEY

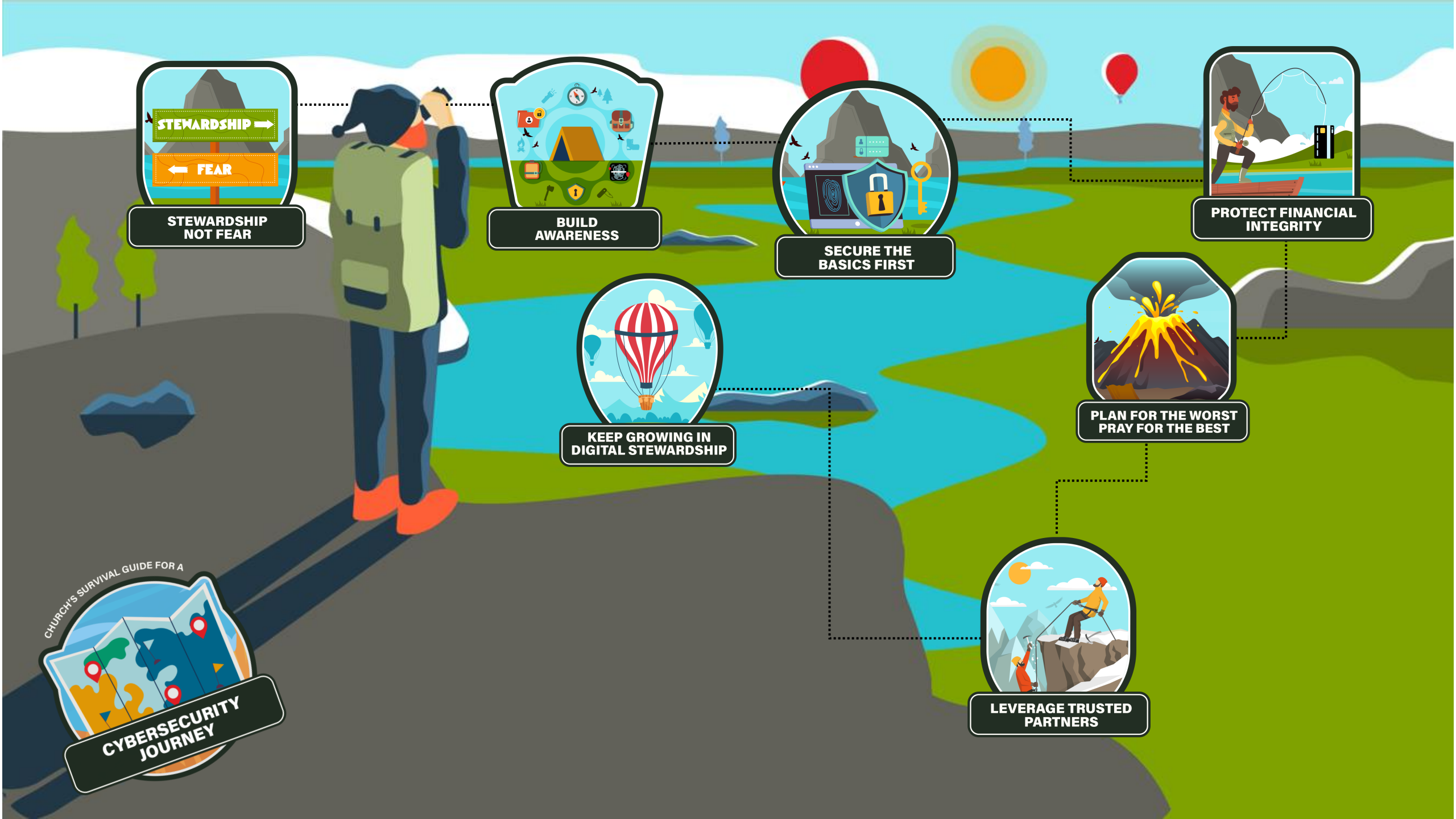
SPEAKER

Lori Baughman

Learning and Development Instructor

CHURCH'S SURVIVAL GUIDE FOR A

CYBERSECURITY JOURNEY


STEWARDSHIP
FEAR
STEWARDSHIP NOT FEAR
BUILD AWARENESS
SECURE THE BASICS FIRST
PROTECT FINANCIAL INTEGRITY
KEEP GROWING IN DIGITAL STEWARDSHIP
PLAN FOR THE WORST PRAY FOR THE BEST
LEVERAGE TRUSTED PARTNERS
CHURCH'S SURVIVAL GUIDE FOR A
CYBERSECURITY JOURNEY

Churches are sacred spaces—but in today's digital world, they're also data hubs. From online giving to livestreaming worship, congregations rely on technology more than ever.

This guide equips church leaders, staff, and volunteers with practical steps to safeguard their mission, protect their people, and steward resources responsibly.

START WITH STEWARDSHIP NOT FEAR

- Cybersecurity is an act of stewardship: protecting the congregation's trust, finances, and reputation.
- Security is part of discipleship—caring for the congregation includes caring for their data.

BUILD AWARENESS ACROSS THE CONGREGATION

- Train staff and volunteers on phishing, password hygiene, and safe device use.
- Would you leave the church doors unlocked overnight? Then don't leave your accounts unprotected.
- Encourage a culture of reporting suspicious emails or activity without shame.

SECURE THE BASICS FIRST

SECURE THE BASICS FIRST

- **Passwords & MFA:** Require strong, unique passwords and enable multi-factor authentication (MFA) on all accounts.
- **Device Updates:** Keep church computers, tablets, and phones updated.
- **Backups:** Regularly back up financial and membership data to secure, offsite storage.

- Wi-Fi: Separate guest Wi-Fi from staff/admin networks.
- UMC Support – GCFA can help you with all these tasks.

PROTECT FINANCIAL INTEGRITY

- Safeguard online giving platforms with MFA and vendor due diligence.
- Reconcile accounts monthly and monitor for unusual activity.
- Limit who has access to financial systems and credit cards.

PLAN FOR THE WORST
PRAY FOR THE BEST

- Create an Incident Response Plan: Who do you call if accounts are hacked or ransomware hits?
- Document key contacts (IT support, vendors, insurance, denominational resources).
- Run tabletop exercises with staff—practice what you'd do in a breach.

LEVERAGE TRUSTED PARTNERS

LEVERAGE TRUSTED PARTNERS

- Work with denominational IT teams, local cybersecurity professionals, or vetted vendors.
- Use tools like KnowBe4 for awareness training and Microsoft 365/Google Workspace security features.
- Don’t reinvent the wheel—adapt best practices from nonprofits and small businesses.

KEEP GROWING IN DIGITAL STEWARDSHIP

- Encourage ongoing learning: short trainings, newsletters, or “cyber moments” in staff meetings.
- Celebrate wins—when someone reports a phishing attempt, thank them publicly.

CHURCH'S SURVIVAL GUIDE FOR A

CYBERSECURITY JOURNEY

STEWARDSHIP NOT FEAR

BUILD AWARENESS

SECURE THE BASICS FIRST

PROTECT FINANCIAL INTEGRITY

PLAN FOR THE WORST PRAY FOR THE BEST

LEVERAGE TRUSTED PARTNERS

KEEP GROWING IN DIGITAL STEWARDSHIP

SURVIVAL CHECKLIST

SURVIVAL CHECKLIST

- [ ] Strong Passwords changed every 90 days
- [ ] MFA enabled on all accounts
- [ ] Backups taken regularly, move things to Cloud (M365 or Google)
- [ ] Staff and congregation trained on phishing scams (KnowB4)
- [ ] Incident response plan documented
- [ ] Vendor security reviewed
- [ ] Financial systems regularly monitored
- [ ] Guest Wi-Fi separated out

Cybersecurity isn’t just about technology—it’s about trust.

By taking intentional steps, your church can continue its mission with confidence, knowing it is protecting the people and resources God has entrusted to its care.

PANEL DISCUSSION

Sharon Asmus
Chief Information Officer

Rob Jett
Technology Services Manager

TECHNOLOGY VALUE PACK!

Protect your ministry. Simplify your tech. Gain peace of mind.

Essentials Cybersecurity

24/7 monitoring, antivirus, and data backup to keep your computers and ministry files protected.

Service Desk Support

Access to our IT team for help with software, connectivity, or device issues.

Advanced Security

Protection from phishing and email scams, password management, and intrusion prevention.

Scan QR code or email connectionalrelations@gcfa.org to get started!

THANK YOU!

For more information visit:

https://www.gcfa.org/technology-support-services

UMC INFORMATION TECHNOLOGY SUPPORT