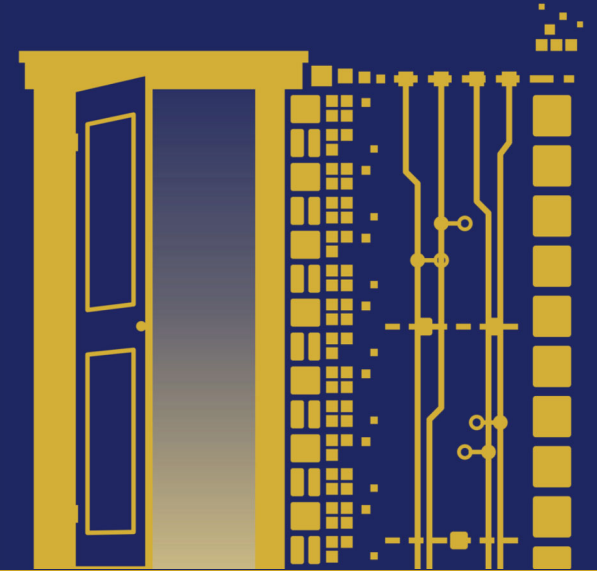


# Guarding the Gates

Cybersecurity as a Ministry of Stewardship



Dr. Laura A. Jones

Ph.D. | MSQSM | CISM | CRISC | CGEIT | CC | PMI-RMP | PMP

October 26, 2026



*Generations of church leaders have been entrusted  
with safeguarding what matters most—  
God's people.*

*Today, that responsibility extends into the digital world, where much of the information,  
communication, and ministry leaders care for now lives.*



# Access Was Primarily Local, Visible, and Physical



Access was bounded by three physical realities:

## **PLACE**

**You had to be on-site.**

Entry meant crossing a visible threshold.

## **PEOPLE**

**Keys belonged to known people.**

Ushers and leaders could see who entered.

## **TIME**

**Doors closed at a known time.**

Activity happened during known hours.

## **The perimeter was tangible.**

Doors • locks • windows • gates • lighting • cameras



THE NEW LANDSCAPE – HYBRID, INTERCONNECTED, AND COMPLEX

# Today's Access Is Internet-Based and Borderless

## WHAT IS NOW AT RISK

| People | Reputation | Data | Identity | Trust | Financials | Worship Services |
|--------|------------|------|----------|-------|------------|------------------|
|--------|------------|------|----------|-------|------------|------------------|

## WHERE IT NOW LIVES

|                        |                             |                       |
|------------------------|-----------------------------|-----------------------|
| Member records         | Giving platforms            | Livestreams           |
| Children's information | Email/SMS messaging         | Payroll               |
| Counseling information | Websites                    | Social media          |
| Donor information      | Cloud and internet services | Care ministry records |

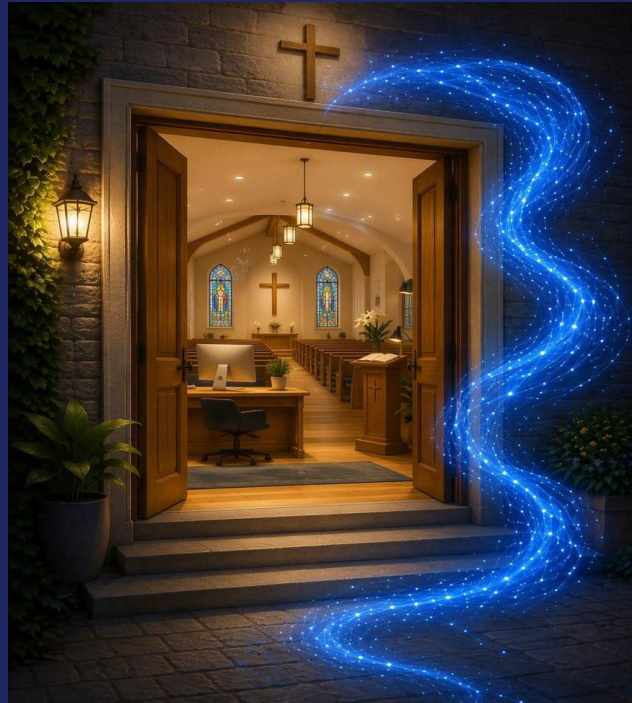




# The Serpent Has Gone Digital

- Deception isn't new
- Impersonation isn't new
- Theft isn't new
- Abuse of trust isn't new
- Manipulation isn't new

*What has changed is the medium.*



*How it shows up today:*

Phishing

Deepfakes and impersonation

Social engineering

Fraudulent requests

Account takeover

Misinformation

Insider threat/misuse

*"...for we are not ignorant of his devices." - 2 Corinthians 2:11 (KJV)*



# Real Churches, Real Lessons

*Four publicly reported incidents, drawn from breach filings, diocesan statements, and ransomware leak-site tracking*

## Diocese of Salisbury/Church of England

Jul–Aug 2025

A cyberattack on the software supplier (Intradev) of background-check provider APCS, c. 31 Jul 2025, exposed DBS applications from Dec 2024–May 2025. Experian monitoring offered; reported to the ICO.

**Key Takeaway:** A vendor's breach can impact your operations.

## New Beginnings Church (NC)

Jan 27, 2026

The INC Ransom group claimed the attack on its leak site. No ransom amount disclosed.

**Key Takeaway:** No congregation is too small to target.

## Chapel Hill Presbyterian Church (WA)

Jan 30, 2026

Unauthorized external access; about 1,000 individuals notified, with filings in several states. No data types or costs disclosed.

**Key Takeaway:** A small breach can still trigger multistate notices.

## First United Methodist Church, Boerne (TX)

May 11, 2026

The Interlock group claimed the attack and claimed to have leaked staff, member, and children's data. No ransom figure disclosed.

**Key Takeaway:** Stolen data can be weaponized, not just locked from intended use.

Sources: Ransomware.live, DeXpose, UpGuard, Church Times, Diocese of Salisbury, Maine and Massachusetts AG breach filings



# Limited Data Does Not Mean Lack of Cyber Risk

*Churches do not need to be favored targets to be easy ones*

## 2nd

The NGO sector ranks second among targets of cybercriminals and hackers, behind only IT.

## 70%

of NGOs have no in-house incident response, analysis, or investigative capability.

## ~85%

of reported U.S. cybercrime losses in 2025 came from cyber-enabled fraud.

Financial losses tied to most cyberattacks on churches remain largely undisclosed.

Limited disclosure may leave an information gap. That doesn't mean the risk is absent.



# Church and Corporate Culture are Similar

*Our greatest strengths can become vulnerabilities*

*"They've shown good character; there is little concern."*

**Excessive trust**

*"Let's give them full access so they're not held up."*

**Privileged access**

*"Just send it to me."*

**Informal information handling**

*"Hackers are focused elsewhere."*

**False sense of security**

Trust without consistent and proper verification can become a vulnerability.



# Guarding the Money Gate

*Business email compromise needs only a trusted name and a willing hand*

**\$20B+**

in reported U.S. cybercrime losses  
in 2025, a record high.

**\$3B+**

lost to business email  
compromise in 2025.

**22,000+**

FBI complaints in 2025 referenced  
artificial intelligence.

## Security controls finance leaders may already be using:

Calling back on a known number before fulfilling an unexpected request • Mandating two approvers for wires and ACH • Assessing vendors for risk before using them (e.g., *Normal Risk*, *High Risk*, *Critical Risk*)

Ask your finance team: How do we verify a request to change where money goes?



# What You Are Really Protecting

*It's much less about the servers...the networks...the computer*



## The congregation

Making online donations;  
submitting health-related  
prayer requests



## The family

Receiving counseling;  
generationally records



## The child

Registering for  
youth services



## The employee

Providing banking details  
for payroll



## The guest minister

Sharing personal and travel  
details

Cybersecurity looks different when we remember that behind every record is a person



# Biblical Narratives Already Discuss Risks



## Temptation and the Fall

*Social Engineering and Deception*



## Guard Your Heart

*Vigilance & Access*



## Jacob Impersonating Esau

*Identity theft, impersonation, and scams*



## Judas as the Moneybag Keeper

*Insider threat*



## Misrepresented Truth

*Data integrity & misinformation*



## The Tree of Knowledge

*Principle of least privilege*



## Decisions and Actions

*Audit & Accountability*

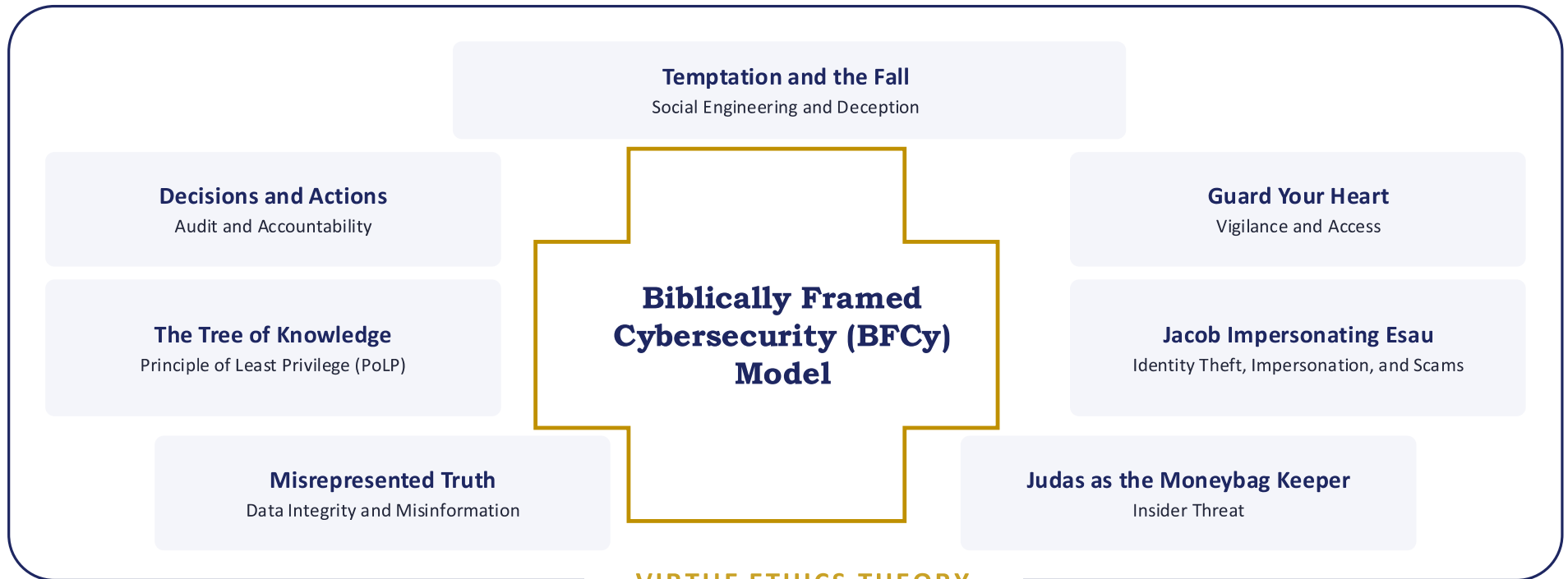


## THE CENTERPIECE

# Introducing the Biblically Framed Cybersecurity Model

## DIVINE COMMAND THEORY

*Regulation, Guidance, and Documented Expectation Setting*



## VIRTUE ETHICS THEORY

*Character and Principled Behavior*

*Model source: Jones, L. A. (2025). Businesses, 5(4), 60.*



## SEVEN STEWARDSHIP PRINCIPLES

# Principle Meets Practice

| Principle                                                                                                                            | Effective Stewardship Indicators                                                                                                | Cybersecurity Practice                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
|  <b>Stewardship</b><br><i>1 Corinthians 4:2</i>     | We know what has been entrusted to us, and we protect it.<br>Risks are identified, understood, and actively being reduced.      | Inventory and risk assess critical assets                                              |
|  <b>Vigilance</b><br><i>1 Peter 5:8</i>             | Digital threats are monitored before harm occurs.<br>Digital doors are watched as carefully as physical ones.                   | Monitoring and verification against social engineering and impersonation               |
|  <b>Integrity</b><br><i>Proverbs 11:3</i>           | The information and systems guiding our decisions can be trusted.                                                               | Data integrity controls and checks against misinformation                              |
|  <b>Accountability</b><br><i>Romans 14:12</i>       | We know who has access and what they are doing.<br>Ownership is assigned for the areas that matter most.                        | Least privilege, access reviews, and audit trails against insider and external threats |
|  <b>Justice</b><br><i>Micah 6:8</i>                 | We honor our obligations to the people whose information we hold.<br>If harm occurs, we promptly and appropriately notify them. | Breach notification and privacy obligations to the people affected                     |
|  <b>Resilience</b><br><i>Proverbs 24:16</i>         | The ministry can recover if something significant goes wrong.<br>The resources needed in a crisis are identified and available. | Backups, continuity plans, and incident response                                       |
|  <b>Shared Responsibility</b><br><i>Nehemiah 3</i> | Roles are understood in protecting the church.                                                                                  | Training and a security-aware church culture                                           |

The seven principles extend the published BFCy model into governance practice. Risks named in the right-hand column come from the model (slide 12).



## BEYOND THE TECHNICAL CONTROLS

# Cybersecurity Must Be a Part of Daily Operations

*Culture turns security from a technical requirement into a shared habit*



Security isn't only about technology and physical devices.

Security is amplified when people understand that protecting one another is part of how the church cares for its community.



# Five Questions Every Church Leader Should Ask

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**

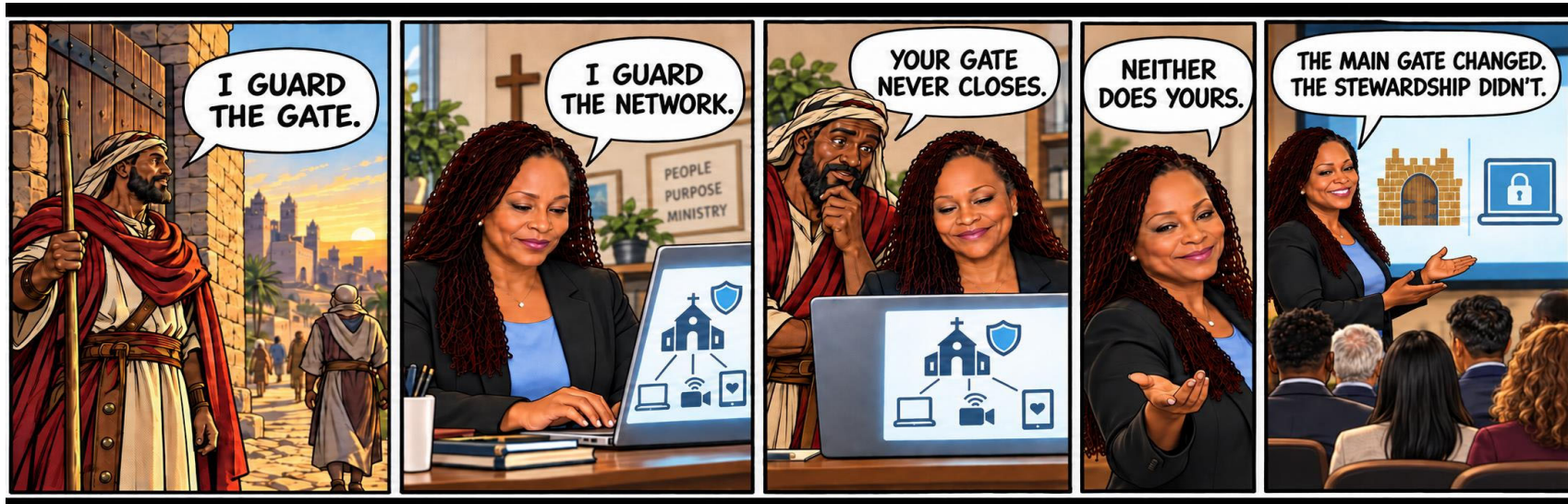
5 How would we know if someone were impersonating one of our leaders?

**VIGILANCE**



# Access Changed – Not the Mission of Stewardship

Vigilance. Protection. Stewardship.





# How to Get Started

## THIS WEEK

Ask the five questions with your leadership team.

## OVER THE NEXT MONTH

Name an owner for each of your digital gates.

## THIS QUARTER

Rehearse how ministry continues if systems go down on a Sunday.

---

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



A church organization might not be subject to a regulation stating,  
“Every church shall maintain a cybersecurity risk management program...”

**But that does not mean it has no legal or contractual obligations for the information entrusted to it.**

---

**Examples:** breach-notification laws • state privacy laws • PCI DSS v4.0.1 for card giving (contractual) • payroll records

*Guarding the Gates isn't about becoming cybersecurity experts.*

**It's about good governance and stewardship.**

THANK YOU



# Dr. Laura A. Jones

Cybersecurity risk and governance leader | Researcher | Educator

## 21 years

U.S. Army service, retired Master Sergeant

## 2 Ph.D.s

Cyber Leadership and Product Management

## 40+

Peer-reviewed publications on  
cybersecurity, AI, and risk

## Executive coach

Carnegie Mellon Chief Risk Officer program



*Let's continue the conversation*

**[DrJones@STEMulateMinds.com](mailto:DrJones@STEMulateMinds.com)**

Atlanta, GA