Jones, Laura A.

Article

Guarding the gates: Exploring a theological-philosophical framework for cybersecurity and spiritual discernment in the digital age

Businesses

Provided in Cooperation with:
MDPI – Multidisciplinary Digital Publishing Institute, Basel

Suggested Citation: Jones, Laura A. (2025) : Guarding the gates: Exploring a theological-philosophical framework for cybersecurity and spiritual discernment in the digital age, Businesses, ISSN 2673-7116, MDPI, Basel, Vol. 5, Iss. 4, pp. 1-31, https://doi.org/10.3390/businesses5040060

This Version is available at:
https://hdl.handle.net/10419/338826

businesses

MDPI

Opinion

Guarding the Gates: Exploring a Theological–Philosophical Framework for Cybersecurity and Spiritual Discernment in the Digital Age

Laura A. Jones

Department of Cybersecurity, Capitol Technology University, Laurel, MD 20708, USA; lajones@captechu.edu

Abstract

This paper examines the intersection between Christian theological principles and contemporary cybersecurity challenges, with a focus on the specific vulnerabilities and responsibilities of faith-based organizations. Recognizing that digital threats emerge not only from technological weaknesses but also from human motives and ethical failings, this study introduces a Biblically Framed Cybersecurity (BFCy) Model that integrates scriptural ethics with established security practices. Through a narrative literature review and comparative analysis, the research synthesizes Christian concepts, such as stewardship, vigilance, and integrity, with technical standards (including the CIS Controls v8, NIST CSF 2.0, and ISO 27001:2022), mapping biblical narratives to contemporary risks like social engineering, insider threats, and identity theft. The findings underscore that robust cybersecurity requires more than technical solutions; it also demands a culture of moral accountability and spiritual awareness. Practical recommendations, including tables linking biblical values to operational controls, highlight actionable steps for church leaders and faith-based organizations. This study concludes that effective cybersecurity in these contexts is best achieved by aligning technical measures with enduring ethical and spiritual commitments, offering a model that may inform religious and broader organizational approaches to digital risk and resilience.

Keywords: cybersecurity; Christian ethics; interpersonal deception theory; religious organizations; parallelism; trust theory

Academic Editor: Daniel Badulescu

Received: 30 July 2025
Revised: 11 October 2025
Accepted: 20 October 2025
Published: 13 December 2025

Citation: Jones, L. A. (2025). Guarding the Gates: Exploring a Theological–Philosophical Framework for Cybersecurity and Spiritual Discernment in the Digital Age. *Businesses*, *5*(4), 60. https://doi.org/10.3390/businesses5040060

1. Introduction

Cybersecurity concerns continue to intensify as technology, human behavior, and ethical considerations converge (Burton & Moore, 2024; Kure et al., 2022; Saeed et al., 2025). These concerns are likely to continue escalating because of global interconnectivity and the emergence of new technologies. As systems become increasingly reliant on digital platforms, the challenges involved in safeguarding these systems escalate alongside the dangers arising from human behavior (Nobles, 2022; Nobles & Burrell, 2024) and technological factors (Burton & Moore, 2024; Jones & Burrell, 2025; Shadbad, 2021).

The rapid pace and increasing sophistication of cyber threats pose individuals and organizations with ever greater challenges in safeguarding their information, systems, and trust. Cyber risk arises from sociotechnical systems characterized by the interdependence of human behavior and technology. The two parts are fundamentally interconnected, especially within faith-based groups. According to the Ponemon Institute's (2023) Cost of Insider Risks Global Report, organizations are increasingly recognizing the key role that

artificial intelligence (AI) and machine learning play in thwarting insider threats. According to the report, 64% of the respondents to a survey stated that technologies played an essential (33%) or significant (31%) role in preventing, investigating, escalating, containing, and remediating incidents originating within their organizations. These responses represent a notable increase from the 54% of organizations that held this belief in 2022. Additionally, 61% of the respondents indicated that automation is very important (38%) or crucial (23%) for managing internal threats within an organization.

The emergence of ethical dilemmas, human factors, and imminent threats necessitates robust cybersecurity measures (Jones, 2024). The cybersecurity industry is anticipated to expand significantly (Saeed et al., 2025), with an overall growth of $5.7 trillion (69.94%) from 2023 to 2028 (Petrosyan, 2023). Furthermore, global cybersecurity expenditures are anticipated to reach $124 billion (Petrosyan, 2022). Given the heightened and irreversible reliance on technology, companies must safeguard the assets essential to operational continuity and overall success (Kure et al., 2022).

Exploiting vulnerabilities through social engineering often involves manipulative, dishonest tactics with significant consequences. According to the FBI, the costs associated with cybercrime reached at least $16 billion in 2024 (Reuters, 2025). Cybersecurity risks vary depending on the nature of the attacks and the vulnerabilities of the assets being targeted. The threat of cyber warfare is a significant concern for corporations, governments, and even charitable organizations such as churches and other nonprofit institutions. In 2023, the average global cost of a data breach was $4.45 million, with sizeable repercussions for industries such as healthcare and finance. Therefore, no organization dependent on the internet is impervious to cybersecurity threats (IBM Security, 2023; Jones, 2021). Likewise, the employees of organizations create vulnerabilities (Nobles & Burrell, 2024; Nobles, 2022).

Thus, although security protocols establish the basis for digital protection, most breaches arise from human vulnerabilities, including deception, betrayal of trust, failure to verify, and the omission of necessary protective measures (Nobles & Burrell, 2024; Nobles, 2022). Every religion involves a doctrine and, in many cases, sacred texts that delineate the beliefs and obligations of its followers (Alkhouri, 2024; Renaud & Dupuis, 2023). Amid the variation among religions and their subdivisions (e.g., Catholic and Protestant Christians), religious groups and denominations typically reach a consensus on their doctrines and behavioral standards.

Subsequently, religious protocols have been established and ratified over time (Alkhouri, 2024; Renaud & Dupuis, 2023). As risks escalate, the need for ethical clarity and discernment becomes paramount (Ephesians 5:15–17 (New International Version, 2011); Jones, 2021; Philippians 1:9–10), especially in organizations that consider trust, stewardship, and accountability essential to their mission. Faith-based institutions, which often operate with inadequate cybersecurity infrastructure, are not exempt (Alkhouri, 2024), as they are increasingly becoming targets due to their financial assets, the personal data they collect, and their inherently trusting nature.

A unique combination of organizational, cultural, and technical factors makes religious institutions and faith-based organizations increasingly susceptible to cyberattacks (Cybersecurity and Infrastructure Security Agency, 2023). Although churches may seem to lack high-value targets, they frequently handle significant amounts of sensitive data, including donor information, financial records, membership databases, and pastoral counseling notes, rendering them "data-rich" (Cybersecurity and Infrastructure Security Agency, 2023; Troilo et al., 2017). However, these institutions often have limited resources to protect their sensitive digital assets (CyberPeace Institute, 2023). Numerous entities lack dedicated cybersecurity staff, robust technical infrastructure, and established strategies to protect these assets (Jones, 2021; Nobles & Burrell, 2024). As a result, they are "defense-poor,"

lacking the requisite layered security to counter the increasingly sophisticated cyberattacks (Pattison-Gordon, 2022).

The theological aspects of trust, truth, and moral responsibility, particularly in Christianity, provide a context for recognizing, preempting, and addressing cyber deception. Analogous to the biblical warning about wolves in sheep's clothing (Matthew 7:15), modern cyber attackers masquerade as legitimate entities to exploit human kindness (Nobles, 2022; Nobles & Burrell, 2024). Social engineers, fraudsters, and insider threats often impersonate credible individuals (Jones, 2021), such as coworkers, supervisors, suppliers, and intimate partners, to exploit trust for personal or organizational gain. Their effectiveness in this regard depends not on brute force but on psychological manipulation, ethical compromise, and trust-exploitation dynamics that scripture continually cautions against (Renaud & Dupuis, 2023).

This research applied biblical teachings to cybersecurity, and similar parallels concerning deceit and ethical consequences can be found in other religious and philosophical traditions (Alkhouri, 2024; Renaud & Dupuis, 2023). The Christian tradition offers a comprehensive moral framework for Christians, grounded in principles such as discernment, stewardship, repentance, and the cognizance of humanity's fallen nature, which can facilitate efforts to address the ethical challenges posed by technology. However, atonement and forgiveness are attainable, while ethical cybersecurity entails adhering to regulations, acquiring knowledge, being accountable, and advancing morally. Biblical texts suggest that efforts to address issues such as cybersecurity should not assume universal perfection, but rather a pragmatic consideration of human nature. Good stewardship entails accountability for the resources entrusted to individuals, including data and technology, within the biblical framework of stewardship. Individuals must exhibit honesty and transparency, for concealing issues and blaming others are inconsistent with professional ethics.

This study aimed to examine ethics and moral vigilance as essential components of technical security systems by assessing cybersecurity threats through the lens of Christian theology, especially in an era characterized by increasing human-centered vulnerabilities. Cybersecurity need not be confined to algorithms (Nobles & Burrell, 2024; Nobles, 2022) but may also encompass spiritual integrity, ethical culture, and the development of wisdom. By employing scripture-informed judgment, individuals and organizations can enhance their resilience against technical exploitation while preserving moral clarity in a complex digital era (Renaud & Dupuis, 2023).

Key takeaways of this section emphasize that cybersecurity threats are escalating due to the convergence of technology, human behavior, and ethical complexities, particularly in globally interconnected environments and faith-based groups. Organizations face increasing challenges from sociotechnical risks, including insider threats and social engineering that exploit human vulnerabilities and trust, necessitating robust technological safeguards and ethical clarity. Faith-based institutions, which are often "data-rich but defense-poor," require prudent stewardship and discernment rooted in biblical principles, as theological values like trust, honesty, and accountability frame effective responses to cyber deception. Ultimately, moral vigilance and spiritually informed judgment complement technical controls, empowering organizations to fortify resilience and preserve ethical integrity amid evolving cyber risks

2. Statement of the Problem

Corporations and religious institutions are increasingly vulnerable to external and internal threats. Victims may be exploited by schemes such as pig butchering scams, wherein perpetrators cultivate trust through attentiveness and empathy and persuade their victims to relinquish money or assets with promises of rewards (Burton & Moore, 2024). Organiza-

tions may be compromised by "organizational arsonists," individuals who instigate turmoil, conflict, and dysfunction to further personal goals, acquire power, or influence narratives (Burton, 2025; Jones, 2024; Jones & Burrell, 2025). As mentioned, in 2024, the global cost of cybercrime was approximately $16 billion (Reuters, 2025), with social engineering and deception-based attacks accounting for around one-third of data breaches (Verizon, 2023). Notably, approximately 95% of breaches are attributable to human error or insider activity (World Economic Forum, 2022). In 2023, schemes such as pig butchering resulted in at least $3.8 billion in recorded losses (Burton & Moore, 2024). Despite this empirical evidence, most organizational remedies are primarily technical, offering limited solutions to address the risks posed by human motivations, ethical blind spots, and value conflicts (Nobles, 2022; Nobles & Burrell, 2024). In 2024, around 30% of religious institutions experienced various types of cyberattacks. Nonprofit organizations, including faith-based institutions, now represent the second-most-targeted sector by cyber attackers, comprising 31% of all notifications about nation-state assaults (CyberPeace Institute, 2024; Department for Science, Innovation and Technology, 2025). While comprehensive statistics on cyberattacks against religious institutions are limited, the recorded occurrences and increasing trend underscore the pressing need for enhanced cybersecurity in these institutions.

3. Significance, Importance, and Novelty of the Inquiry

The intersection of religious beliefs and cybersecurity practices is a complex dynamic that influences individuals' behavior and cognition in the online and spiritual domains alike (Alkhouri, 2024). For Christians, the Bible is the primary source of spiritual, moral, and practical wisdom (2 Timothy 3:16–17; John 3:16; Psalm 119:105). Given the relevance of biblical writings to Christians, valuable insights from this wisdom apply to fields such as cybersecurity, fraud detection, and deception analysis. Thus, this study takes a Christian theological perspective rooted in biblical ethics.

Various chapters and teachings in the Bible are pertinent to modern organizational resilience when analyzed in light of their fundamental messages (Alkhouri, 2024). So, while the Bible does not, of course, mention phishing or malware, it does explore essential themes such as temptation, deception, misplaced trust, and the consequences of erroneous judgment. The discussions of dishonesty, trust, alertness, and ethical compromise in the Bible are highly relevant to modern cybersecurity. This concept paper presents a critical analysis of various biblical narratives and teachings pertinent to cybersecurity, integrating theological and philosophical viewpoints.

The swift evolution of cybersecurity risks poses significant challenges (Cybersecurity and Infrastructure Security Agency, 2023; Office of Intelligence and Analysis, 2025), but fundamental concepts concerning cyber safety, especially alertness, trustworthiness, integrity, and the repercussions of misconduct, align with enduring biblical teachings (Alkhouri, 2024; Renaud & Dupuis, 2023). The gap between these swiftly increasing threats and the frequently neglected notion of lasting comprehension is significant. This raises the question of how companies and individuals can apply core security principles and ethical norms to address and mitigate the challenges posed by the modern threat landscape (Burton & Moore, 2024; Nobles & Burrell, 2024). Businesses must avert the digital equivalent of the Fall of Man, as described in Genesis 3:1–24, by securing themselves against data corruption, trust erosion, and societal harm in a modern context.

This inquiry presents strategies for proactively mitigating the hazards caused by cyber vulnerabilities based on the responses to and safeguards against malevolent intentions described in the Bible (Alkhouri, 2024; Ephesians 6:11–13; Psalm 119:9–11). Burton and Moore (2024) argued that contemporary pig butchering scams exemplify extended social engineering. Victims are gradually manipulated into trusting relationships that lead to

financial and psychological exploitation (Burton & Moore, 2024; Ohu & Jones, 2025a, 2025b). In like manner as the serpent presents Eve with ostensibly beneficial knowledge, cybersecurity fraudsters may offer illusory investment returns and promises of amorous satisfaction (Genesis 3:13; Paul et al., 2023).

The theological conclusion is significant: deception leads to brokenness when individuals place their trust in false promises rather than truth. Therefore, organizations and individuals must cultivate technological safeguards and spiritual discernment. God has demonstrated the importance of security measures since the beginning of time (Genesis 3:24; Ephesians 6:11–13; Exodus 25–27; Nehemiah 4:7–9; Proverbs 2:11, 4:23). This emphasis in the Bible on security measures may prompt Christian leaders to investigate cybersecurity strategies that align with scripture. This investigation underscores concepts firmly rooted in Christianity, but as noted, adjacent theologies could adopt this biblical-cyber perspective.

4. Materials and Methods

This study employed a qualitative, narrative review methodology to investigate how Christian theological principles intersect with cybersecurity practice, particularly in relation to organizational resilience and spiritual stewardship. Primary source materials included key biblical passages from the Old and New Testaments of the New International Version (2011). In contrast, secondary sources comprised peer-reviewed journal articles, books, professional reports, and leading cybersecurity standards, such as CIS Controls v8 (Center for Internet Security, 2021), the NIST Cybersecurity Framework 2.0 (National Institute of Standards and Technology, 2024), and ISO 27001:2022 (International Organization for Standardization [ISO], 2022).

Literature was gathered using systematic keyword searches (e.g., "cybersecurity," "Christian ethics," "religious organizations," "trust theory") in major academic databases, including JSTOR, IEEE Xplore, Google Scholar, and relevant organizational archives. The selection criteria limited sources to English-language publications from 2015 to 2025, with an emphasis on studies and guidelines pertinent to ethical, human-centered digital threat management and faith-based institutions.

The research process involved thematic synthesis, identifying, comparing, and integrating biblical concepts (such as stewardship, vigilance, and integrity) with technical controls and operational practices emerging from the cybersecurity standards and empirical studies. The Biblically Framed Cybersecurity (BFCy) Model was developed by systematically correlating scriptural imperatives with concrete security measures from established frameworks.

5. Discussion

5.1. The Intersection of Technology, Human Nature, and Ethics

5.1.1. Technology

Ecclesiastes 7:29 states, "God made mankind upright, but they have gone in search of many schemes." In scripture, technology, tools, systems, and structure simultaneously serve human progress and rebellion. Thus, in Genesis, humanity is given dominion over creation in a call to stewardship that includes technological innovation to cultivate the world. Later in Genesis 11:1–9, the misuse of a collective technological effort (the Tower of Babel "with its top in the heavens") leads to fragmentation and divine intervention. This event also explains the basis for diverse languages and is often interpreted as a cautionary tale about pride, unity without purpose, and the defiance of divine boundaries.

Leaders in academic theology must acknowledge that no system can be deemed secure if it neglects the possibility of human or technical fallibility, nor should people depend exclusively on technology. Intervention remains essential in advanced technologies,

including AI, artificial general intelligence, and quantum computing. Ecclesiastes 3:11 articulates humanity's yearning for eternity and the transcendent, thereby underscoring humanity's distinctive position in the cosmos.

Fascination and rivalry are essential to technological growth, and efficient security models must consider established conventions, accountability, oversight, and continuous evolution (Nobles, 2022; Nobles & Burrell, 2024). There needs to be a balance between technologies that facilitate easier engagement among people and people's efforts to monitor how technology affects them (Nobles, 2022; Nobles & Burrell, 2024; Shadbad, 2021). Cyber protection is more than just better firewalls. In this context, Colossians 1:17 poses a relevant question about the investment of faith to preserve unity.

5.1.2. Human Nature

Even if technology is flawless, the human component in cybersecurity remains erratic and unreliable. As mentioned, 95% of cybersecurity breaches are attributed to human errors, including susceptibility to phishing schemes, misconfigurations, and social engineering (World Economic Forum, 2022). The technological aspect of cybersecurity constitutes only half of the challenge, for the human element remains a variable that is unpredictable and challenging to forecast and control.

Jeremiah 17:9 presents the profound theological insight that humans are predisposed to self-deception, moral decay, and imprudent choices. This predisposition extends beyond mere spiritual awareness to inform tangible actions in cybersecurity. Scams such as phishing, spear-phishing, and baiting exploit victims' trust, haste, anxiety, and curiosity (Burton & Moore, 2024; Hadlington, 2018; Nobles & Burrell, 2024). Well-disposed employees in organizations can represent a vulnerability, for stress, exhaustion, or resentment may lead an individual to engage in deliberate or inadvertent malevolent conduct (Burton & Moore, 2024; Hadlington, 2018; Nobles, 2022; Nobles & Burrell, 2024; Shadbad, 2021).

No system can completely predict or control this randomness. Multifactor authentication and least-privilege access do not merely account for likely errors but expect them. Training should assume that users are distractible, overconfident, and susceptible to manipulation. Confronting cybersecurity risks involves addressing technical components, such as faulty configurations and flawed code, and establishing controls to guard against humans' flawed nature. Researchers have argued that there is value in learning from the established best practices of other disciplines that also depend on human actions (Renaud & Dupuis, 2023). This is a compelling argument, especially considering that cybersecurity is a relatively young discipline that has yet to address the complexities of human nature and error fully. Other disciplines have decades, if not centuries, of experience addressing problems that arise in modern business when workers deviate from established guidelines and propagate vulnerabilities throughout an organization.

5.1.3. Ethics

Business ethics is not a novel concept. In a study published more than 40 years ago, management expert Peter F. Drucker (1981) acknowledged the significance of ethics in business (Hoffman & Moore, 1982), asserting that it transcends the call for repentance from religious leaders. In business ethics, stakeholders are defined as the individuals, groups, and entities that are affected by or can influence an organization's decisions, actions, or policies (D'Cruz et al., 2022). Business ethics is relevant not only to shareholders and investors but also to a diverse array of entities, including employees, consumers, suppliers, government agencies, local communities, and future generations.

From the perspective of biblical ethics, cybersecurity constitutes not just a problem of safeguarding but also an obligation. Jeremiah 17:9, cited above, acknowledges that

human fallibility involves the ethical responsibility to hold individuals accountable without demanding perfection from them. Organizations must transcend superficial evaluations, focusing on discerning behavioral patterns over time and distinguishing between honest and fraudulent acts. In this verse, the prophet Jeremiah asks, "The heart is deceitful above all things and beyond cure. Who can understand it?"

This inquiry prompts contemporary practitioners to recognize the limitations of technology when it comes to identifying malicious intent. Ethical vigilance, behavioral analytics, and ongoing monitoring are essential to identify patterns that reflect deeper realities obscured by superficial validity. Humanity must not succumb to the despair of a constantly evolving technological cybersecurity landscape. Instead, efforts should be made to establish systems, cultures, and laws that acknowledge and mitigate the inherent flaws in human nature. Biblical ethics posits that human nature is intrinsically flawed, predisposed to greed, rationalization, and short-term thinking, which have obvious implications for cybersecurity. Jeremiah 17:9 and Romans 3:23 illustrate that ethical frameworks cannot rely exclusively on good intentions but must acknowledge the inherent human propensity for failure.

5.2. Cyberattacks on Faith-Based and NGO Institutions (2024–2025)

The cybersecurity vulnerabilities and increased risks identified in faith-based and non-governmental organizations highlight deeper systemic issues pertinent to the manuscript's primary focus on sector-wide threat awareness and resilience. Providing tangible, recent examples of these sector-specific threats underscores the urgency of preventive steps and affirms the necessity of ongoing security focus among administrators, policymakers, and stakeholders.

The following current data and trends evidence the escalating threat of cyberattacks:

- Faith-based organizations and charitable entities remain high-risk targets for cybercrime, with threat levels officially classified as "elevated" since July 2025. National bodies overseeing this sector have advocated for increased vigilance in light of the persistent occurrence of ransomware, phishing, doxing, and similar threats (Office of Intelligence and Analysis, 2025). Global conflicts and domestic extremist activities have increased these risks.
- Faith-based organizations can present attractive targets for perpetrators (Cybersecurity and Infrastructure Security Agency, 2023; Office of Intelligence and Analysis, 2025) due to their limited security measures, high-trust cultures, the availability of the information they collect, and their reliance on volunteers. Recent reports indicate that social engineering, email intrusion, and ransomware are particularly prevalent, utilizing insider threats and digital fundraising platforms as entry points (Burton, 2025; Verizon, 2023).

5.3. Recent High-Profile Incidents Involving Faith-Based and Non-Governmental Organizations

Faith-based and non-governmental groups have increasingly been targets for cybercriminals and ideologically driven threat actors. Recent high-profile breaches have highlighted the vulnerability of these institutions, underscoring the intersection of physical and cyber risks and their potential impact on operational continuity and personal safety. These examples illustrate that even prominent and globally respected institutions are susceptible to sophisticated attacks and targeted abuse. The following are some recent cybersecurity breaches.

- A prominent Catholic publisher, Relentless Church, and the Church of Jesus Christ of Latter-day Saints experienced cyberattacks resulting in the exposure of critical information about members and personnel (The Church of Jesus Christ of Latter-day Saints, 2022).

- A sophisticated cyberattack on the International Committee of the Red Cross (ICRC) in 2022 compromised the personal information of more than 500,000 individuals who depended on its humanitarian services, demonstrating that not even globally esteemed faith-based non-governmental organizations (NGOs) are impervious to such threats (International Committee of the Red Cross, 2022).
- Manifestos and explicit threats targeting individual churches, such as a July 2025 event in Boise, Idaho (Gryder, 2025), underscore a connection between physical and cyber threats, which are frequently driven by ideological motives, with pre-incident indicators prompting law enforcement apprehension.

5.4. Sector-Wide Observations

Recent developments indicate that the cybersecurity landscape for faith-based organizations is marked by intensified targeting and greater susceptibility. Religious institutions, regardless of their size or denomination, face a range of complex risks that highlight the pervasive nature of these challenges across the sector. Incidents of data breaches, ransomware, and ideologically driven attacks highlight systemic concerns that necessitate a collaborative focus from leaders and security experts within this community.

The following examples illustrate the types of cybersecurity concerns currently affecting various faith-based entities:

- Email compromise, the primary attack vector for faith-based and charitable groups, has intensified because of the increased use of digital fundraising tools and platforms (Cyber Command, n.d.).
- From 2024 to 2025, the global incidence of ransomware attacks increased by more than 120%, with churches, ministries, and Christian publications increasingly facing ransom demands, operational disruptions, and data loss (Firch, 2025).
- Nation-state and hacktivist activity is also a concern, for pro-Iranian and other state-affiliated forces, as well as ideologically driven domestic radicals have targeted Jewish, Christian, and Islamic organizations amid the ongoing geopolitical crises.

5.5. International Perspective

These challenges are not limited to religious organizations in the United States, as the following examples indicate. Two international perspectives on cybersecurity challenges are provided:

- Cybersecurity threats are increasingly globalized, with incidents recorded in North America, Europe, Asia, and the Middle East, particularly in the United States, Switzerland, the Vatican, and Israel, including attacks on humanitarian organizations.
- The NGO sector lags in preparedness; thus, 56% of NGOs lack a cybersecurity budget, and around 70% are unprepared to address substantial cyber incidents (CyberPeace Institute, 2024). The tendency for small Christian communities to use donated or outdated equipment and shared or insecure passwords increases their vulnerability.

Table 1 delineates essential global and regional statistics that contextualize the existing cybersecurity landscape, emphasizing the magnitude, prevalence, and repercussions of cyber incidents across various sectors and regions. Note that the table includes quantitative data from differing types of organizations (e.g., NGOs, nonprofits, religious institutions, and faith-based institutions) and geographies. This table consolidates recent statistics on attack prevalence, financial losses, and sector-specific vulnerabilities. It provides an empirical basis for comprehending the urgency and scope of cybersecurity concerns. These data offer critical context for managing organizational risk and justify adopting more resilient, culturally sensitive security methods, particularly in faith-based and mission-driven enterprises.

Table 1. Global and Regional Statistics.

Statistic/Trend	Region	Year	Key Points
NGO: 70% of NGOs lack an established incident response program for cyberattacks program to address cyberattacks (CyberPeace Institute, 2024).	Switzerland/ Europe	2023	73% of NGOs surveyed had insufficient recovery processes and limited dedicated budgets (CyberPeace Institute, 2024).
Nonprofit: Sixty-eight percent of nonprofits participating in the research have experienced a data breach in the past three years (CyberPeace Institute, 2024).	Global	2024	Nonprofits are exploited through cyberattacks and account for a significant portion of breaches (CyberPeace Institute, 2024).
Religious Institution: Cyberattacks on religious organizations have been "sharply rising" since 2020 (SC Media, 2024).	Global	2023–2024	High-profile breaches include those targeting the Vatican, churches in the United States, and Jewish educational sites (SC Media, 2024).
Faith-based Institution: Ransomware and hacking attacks directly targeting faith-based institutions, operations disrupted, donor/member data stolen (Gryder, 2025).	North America/ Europe	2024–2025	Churches, ministries, and humanitarian NGOs affected by incidents with data exposure and costly recovery (Gryder, 2025).

Note. The author of this paper created this table.

Globally, NGOs, including faith-based organizations, face a persistent and intensifying threat environment (CyberPeace Institute, 2024; Gryder, 2025; SC Media, 2024) created by criminal and state-sponsored entities (Cybersecurity and Infrastructure Security Agency, 2023; Office of Intelligence and Analysis, 2025). Recent data sources have confirmed that these institutions are experiencing unprecedented targeting, with attackers exploiting resource constraints, high-trust settings, and digital security deficiencies (Cybersecurity and Infrastructure Security Agency, 2023; Office of Intelligence and Analysis, 2025). The effects are extensive, influencing economics, member confidence, and personal safety, highlighting the pressing need for customized security measures and resource distribution.

The widespread implications of cybersecurity underscore the importance of acknowledging that users, developers, and executives may make poor judgments despite having good intentions. Therefore, controls, accountability, and robust policies are essential. Religious organizations and other NGOs regularly manage substantial financial assets and collect confidential personal data from their followers, but often lack adequate cybersecurity measures and are vulnerable to cybercriminals seeking financial gain (CyberPeace Institute, 2023, 2024; Roberts, 2023). Roberts (2023) characterized religious institutions as appealing targets for cybercriminals because of three factors: (a) they are "data rich, defense poor" (cf. Cybersecurity and Infrastructure Security Agency, 2023; Pattison-Gordon, 2022; Troilo et al., 2017), (b) they typically possess financial reserves, and (c) they are characterized by inherent trust among their members.

5.6. Relevant Theories and Conceptual Frameworks

Divine command theory posits that cybersecurity responsibilities supersede professional duties and are moral imperatives derived from divine authority. Strategies designed to avoid data breaches, mitigate fraud, and protect users' privacy align with moral imperatives against deception, betrayal, and carelessness (Máhrik & Králik, 2024). Cyber transgressions, such as willful insider threats and unethical hacking, may also be regarded

as moral violations of divine will rather than simple malicious intent. Conversely, virtue ethics underscores the cultivation of moral character traits such as honesty, prudence, and courage that are considered fundamental to ethical conduct in cybersecurity. In high-risk or uncertain situations, these traits enable professionals to behave with moral clarity, particularly in the absence of specified constraints. These concepts collectively provide complementary frameworks. Thus, divine command theory emphasizes the sanctity of ethical behavior, whereas virtue ethics prioritizes the development of essential character traits for reliable and responsible cybersecurity practices.

Other pertinent conceptual frameworks are examined here, including Erving Goffman's dramaturgical model, interpersonal deception theory (IDT), moral disengagement theory, and trust theories.

- Erving Goffman's dramaturgical theory likens social life to a theatrical performance wherein individuals perform roles to influence the perceptions of others (Smith, 2016). The "frontstage" refers to public conduct that conforms to cultural expectations, whereas the "backstage" reveals concealed intentions and preparations. For Goffman, identity is malleable and adaptable to social settings (Smith, 2016). In cybersecurity, this concept refers to the techniques employed by hackers to create convincing digital communications, such as phishing emails or romance scams, to exploit victims. The precise identities of the perpetrators remain concealed while they conspire in clandestine forums, crafting narratives and utilizing psychological manipulation covertly. This behavior parallels that of biblical heroes such as Jacob, who plotted covertly before public action. Goffman's paradigm underscores the performative nature of cyber deception, thereby augmenting the contrast between biblical and contemporary acts of dishonesty.
- Interpersonal deception theory (IDT) highlights the fluidity of deception in speech, paralleling biblical accounts that feature conversational trickery (e.g., the serpent and Eve). This amalgamation of interpersonal communication and deception theories provides a comprehensive awareness of deception in interactive contexts (Buller & Burgoon, 1996). In cybersecurity, IDT denotes subversive strategies employed by cyberattackers, such as phishing and social engineering. Establishing these links can enhance the sophistication and precision of cybersecurity analogies. Thomas and Biros (2020) showed that it is feasible to differentiate between truthful and dishonest conduct, with behavioral patterns emerging over time.
- Moral disengagement (Bandura, 1990) elucidates how individuals rationalize unethical conduct, making it especially pertinent to insider threats and ethical violations in cybersecurity. This concept aligns with biblical teachings on the justification of sin, thereby enhancing the theoretical complexity of the discourse on "guarding the gates."

  Trust theories facilitate the systematic comprehension of the components of trust, namely ability, kindness, and integrity (Schoorman et al., 1996), which are crucial in religious and cybersecurity contexts. In theology, reliance on divine character signifies dependence on moral purity, whereas in cybersecurity, trust regulates access, authentication, and risk management. These characteristics reveal weaknesses in human and system interactions and underscore the need for reliable conduct and frameworks. Because trust theory facilitates the evaluation of the trustworthiness of entities, whether divine, human, or digital, it is a practical framework for addressing deceit, identity verification, and ethical congruence in spiritual and technological contexts.

  The following discussion delineates some parallels between biblical narratives and cybersecurity.

5.7. Limitations

While this article offers a robust conceptual foundation, its arguments remain circumscribed by a series of consequential boundaries. These methodological and contextual delimitations, ranging from the singular focus on a Christian paradigm and the absence of empirical validation to the insufficient engagement with technological, legal, and intra-faith complexities, simultaneously testify to the promise and unfinished agenda of this research. Nuanced considerations such as organizational heterogeneity, evolving threat vectors, and the distinct vulnerabilities of marginalized faith communities reveal a landscape far richer and more variegated than a singular theological lens can encompass. By articulating these points of tension and omission, the discourse not only exemplifies scholarly transparency but also charts a forward-looking topography for interdisciplinary research, practical innovation, and deeper engagement at the contested intersection of faith, ethics, and digital security. Each of the following limitations links to the paper's thematic construct, highlighting where additional depth, broader inclusivity, or methodological expansion would substantively strengthen its practical application.

- Christian Paradigm Exclusivity. The study is primarily anchored in Christian theology, which may limit its universal applicability. Limited engagement with non-Christian or secular ethical frameworks may not reveal unique and convergent dynamics in cyber-ethical stewardship that could address cross-cultural generalizability.
- Theological Diversity and Intra-Faith Disputes. Christian denominations and communities differ on many theological, ethical, and interpretive issues. The BFCy Model may not yet fully account for these internal distinctions or disagreements about scriptural application in digital contexts.
- Empirical, Quantitative Validation. The effectiveness of the Biblically Framed Cybersecurity (BFCy) Model in changing behaviors or reducing risk remains unquantified and thus open to further validation. Limitations exist regarding the operationalization of the model.
- Scriptural Analogy. While drawing analogies between biblical narratives and modern cyber threats provides rich theological resonance, it may oversimplify the technical complexities of cybersecurity, necessitating a deeper critical-technical analysis in parallel.
- Organizational Scale and Context. There are limitations in rigorously addressing variations in organizational size, structure, or resources, which could significantly affect the adoption and impact of the current model.
- Consideration for Legal and Regulatory Divergence. Specific legal mandates (e.g., GDPR, HIPAA, or region-specific data privacy regulations) may pose practical challenges for faith-based organizations operating in varied jurisdictions.
- Evolving Threat Vectors and Technological Adaptability. Scriptural principles were not the specific focus in terms of agility in responding to new classes of attack (e.g., polymorphic malware, AI-enabled threats).
- Exploration of Human Factors Outside Theological Context. The study is limited in its consideration of the psychological, cognitive, or social factors that could significantly enhance understanding of cybersecurity behaviors beyond spiritual examination.
- Intersectionality of Diverse Religious Communities. The distinct hazards, resource limitations, and socio-political vulnerabilities encountered by marginalized, minority, or persecuted religious groups in cyberspace are limited in their scrutiny.
- Systematic Framework for Execution and Evaluation. Organizations would need to customize a formal, iterative procedure for assessing the progress, outcomes, and ongoing enhancement of the BFCy Model in organizational practice.

- Key takeaways of this section reveal that faith-based and NGO institutions face a highly intensified and evolving cyber threat landscape, mainly due to resource constraints, high-trust environments, and underdeveloped digital defenses. Theologically rooted models stress that cybersecurity is not merely a technical or professional duty but also a profound moral imperative governed by divine command and the cultivation of virtuous character traits. Psychological manipulation and social engineering tactics are used to exploit organizational structures and individual trust, echoing biblical narratives and sociological frameworks. However, current research is bound by notable limitations, including its exclusive focus on Christian paradigms, absence of broad empirical validation, and insufficient accommodation of organizational, legal, and cross-cultural complexities. This underscores the need for interdisciplinary inquiry and continuous adaptation of ethical and practical frameworks in the realm of digital security.

6. Results

6.1. Cybersecurity Threats and Controls Analogous to Biblical Themes

This discussion focuses on seven cybersecurity analogies to biblical references and lessons. Each biblical account is paired with cybersecurity analogies to offer detailed insight into the shared themes and risks. The following parallels are drawn solely from Christian scripture, but other faiths may offer valuable analogies that are worthy of future exploration, though outside the scope of this model. Table 2 presents a cohesive array of examples demonstrating how biblical narratives reflect modern cybersecurity threats and associated defense mechanisms. By examining these scriptural accounts alongside contemporary digital risks, the table facilitates the extraction of actionable insights that can inform the formulation of successful cybersecurity practices, especially within faith-based contexts. This method highlights the importance of fundamental religious teachings in fostering proactive and ethically sound responses to emerging cyber threats.

Table 2. Biblical Narratives and Analogous Cybersecurity Threats and Controls.

Biblical Narrative		**Cybersecurity Threat and Control Analogy**
1	The Temptation and the Fall	Social Engineering and Deception
2	Guard Your Heart	Vigilance and Access
3	Jacob Imitating Esau	Identity Theft, Impersonation, and Scams
4	Judas as the Moneybag Keeper	Insider Threat
5	Misrepresented Truth	Data Integrity and Misinformation
6	The Tree of Knowledge	Principle of Least Privilege (PoLP)
7	Review of Decisions and Actions	Audit and Accountability

Note. The author of this paper created this table.

Faith-based organizations face several cybersecurity dangers that compromise their operations and confidentiality, while also reflecting patterns and teachings from scriptural texts. By comparing modern cyber occurrences to core scriptural events, the greater relevance and severity of these risks are contextualized in a manner that profoundly connects with religious communities.

The following comparative analysis of biblical narratives and analogous cybersecurity threats and controls illustrates the parallels between specific biblical accounts and current cybersecurity challenges, along with relevant preventative strategies. This analyzes scripture tales alongside contemporary cyber hazards and controls, offering a framework to understand how timeless teachings from religious texts might enhance digital risk management techniques in faith-based enterprises and beyond. The subsequent elaborated

examples illustrate how these similarities might guide and motivate a cohesive response to cybersecurity challenges.

6.1.1. Biblical Narrative 1: The Temptation and the Fall

- Text: Genesis 3:13. "Then the Lord God said to the woman, 'What is this you have done?' The woman said, 'The serpent deceived me, and I ate."
- Event: Eve succumbs to the serpent's attack and is led to defy God's order
- Social Engineering and Deception:
    - Cyber Relevance. Eve's succumbing to the serpent's attack allows for a damaging compromise of humanity (the Fall). The Fall is analogous to social engineering: an attacker (the serpent) uses trust and curiosity to drive behavior.
    - Data-backed Insight. Social engineering attacks have been among the most common causes of non-insider data breaches, accounting for 53% of such incidents (Ponemon Institute, 2023).
    - Critical Synthesis. In Genesis, the serpent convinces Eve to eat from the forbidden tree by questioning her comprehension of God's order and offering her hidden knowledge. Persuasion, false promises, and manipulation also entice Eve. The sin (failure), loss of innocence, and awareness of Eve's and Adam's vulnerability have momentous consequences (Genesis 3:13). This account is a timeless example of psychological manipulation, with the assailant exploiting curiosity, trust, and the need for empowerment. Today's attackers employ many of the tactics used throughout the ages, so a coordinated response to malicious activity is still needed (Burton, 2024). Cyber attackers deceive victims by convincing them to violate established norms that help ensure safety, security, resilience, and strategic survivability. In like manner, Adam and Eve realize their mistake too late and attempt to conceal their wrongdoing once they become aware of their mistake. Employees are expected to operate according to established conventions communicated through managerial, administrative, and technical controls, and thus are required to report errors, when necessary, rather than hiding them (Jones, 2024). However, as the experience in the Garden of Eden shows, it is not inconceivable or even uncommon for human curiosity to prevail over expectations.

6.1.2. Biblical Narrative 2: Guard Your Heart

- Text: Proverbs 4:23. "Above all else, guard your heart, for everything you do flows from it."
- Event: The exhortation to diligently guard one's heart.
- Vigilance and Access:
    - Cyber Relevance. When protecting the body, protection of the heart is the most vital task because it is the foundation of everything that defines life. The heart is central to sustaining life. In cybersecurity, controlling access is crucial because organizations must persistently defend the core of their operations and valuable assets, as their status influences the overall integrity of the system.
    - Data-backed Insight. Eighty-four percent of organizations have experienced an identity-related breach, and 96% believe that these breaches could have been prevented with better identity-focused security measures (Identity Defined Security Alliance, 2023).
    - Critical Synthesis. Guarding the heart involves being mindful of what individuals allow into their minds and what influences their inner selves. Likewise, who or what is provided with access to a network directly influences its condition and assurance. Like a fundamental tenet of security design, Proverbs 4:23 emphasizes

proactive protection. Those with authorized access who are entrusted with elevated privileges may make mistakes or abuse trust. In addition, workers often inadvertently provide credentials to attackers owing to a lack of awareness or verification (Hadlington, 2018; Nobles & Burrell, 2024; Triplett, 2022), thereby giving assailants access to parts or all of an organization's network. Systems must be constructed with the defense-in-depth security strategy to safeguard the core from unauthorized access. A single data breach can lead to a 7.5% decline in customer trust and brand reputation (Harvard Business Review, 2023; IBM Security, 2023), with recovery taking years (Roering, 2014). Just as protecting the heart is important for an individual's spirit and morals, protecting identity and access systems is key to strong cybersecurity. Breaches often happen because access controls are ignored, while being careful at the center stops large-scale digital problems. Activities such as following prescribed policies and guidance, seeking clarification, and maintaining cybersecurity awareness mimic the biblical call to spiritual vigilance.

6.1.3. Biblical Narrative 3: Jacob Imitating Esau

- Text: Genesis 27:1. "When Isaac was old and his eyes were so weak that he could no longer see, he called for Esau, his older son, and said to him, 'My son.' 'Here I am,' he answered."
- Event: Jacob uses disguise (imposter risk) and manipulation (trickery) to receive his father's blessing, which is intended for his brother, Esau.
- Identity Theft, Impersonation and Scams:
    - Cyber Relevance. Today's cyber landscape is replete with methods for impersonating identities, including fake social media profiles, phishing attacks, business email compromise, deepfakes, spoofing, and synthetic (combining real and fake information) identity fraud. This kind of identity theft occurs when someone pretends to be someone else to scam individuals for their benefit.
    - Data-backed Insight. Ninety-five percent of breaches have been attributed to human error (Mimecast, 2025).
    - Critical Synthesis. This incident highlights the dangers and magnitude of loss associated with inadequately verifying an identity. Jacob is able to scam his father, Isaac, because Isaac's eyesight (awareness) fails him. While Isaac touches Jacob's hands and neck to ensure that he is blessing Esau (the rightful son, who is authorized to receive the blessing and whose skin is hairy), Isaac's authentication process is thwarted by Jacob's scam. In this situation, Jacob presents a false positive by covering himself with goat hair. The multi-factor authentication process fails as the first control (something known provides recognition on sight, a human factor), and the second control (a physical attribute, i.e., fake hairy skin) is not authentically validated but assumed so. Isaac is completely duped, and Jacob maliciously steals Esau's blessing.
    - The application of this learning to cybersecurity illustrates the critical need for genuine authentication measures to avoid identity theft, impersonation, and scams. In the cybersecurity realm, credential theft incidents have averaged $679,621 per incident (Ponemon Institute, 2023). The goal of credential thieves is to steal users' credentials, which provide access to critical data and information. Further, adverse insiders have accounted for an average of 6.2 incidents experienced between early 2022 and early to mid-2023, and the median cost for such incidents was calculated to be $701,500 (Ponemon Institute, 2023). The people, processes, and

technologies of organizational systems can be exploited if confidence is gained without the use of proper controls.

6.1.4. Biblical Narrative 4: Judas as the Moneybag Keeper

- Text: John 12:6. "God made mankind upright, but they have gone in search of many schemes."
- Event: Judas uses his role and access to help himself to funds in the communal bag.
- Insider Threat:
    - Cyber Relevance. As keeper of the money bag (also referred to as the money box), Judas is an insider threat. He operates inside the system deliberately, using his role-based access for personal gain.
    - Data-backed Insight. Sixty percent of security breaches involve insiders (IBM Security, 2023).
    - Critical Synthesis. Betrayal is conceivable even in close circles, and the legal dimensions of insider threats are vast and multidimensional (Jones & Burrell, 2025). Hence, zero-trust models are especially important. There is growing empirical evidence connecting the psychological profiles of internal and external threat actors to the so-called "dark triad" of personality traits, namely Machiavellianism, narcissism, and psychopathy (Ohu & Jones, 2025b). Just as Judas was the keeper of the money box, individuals entrusted with managing organizational assets can willfully misuse possessions and hide evidence of doing so. Insider threats involve people who work for an organization and have a propensity to engage in actions that expose or misuse information; thus, they pose serious challenges to contemporary businesses (Jones, 2024). Insiders are assigned credentials that allow access to assets, so their responsibilities can carry financial, operational, reputational, and other risks. Organizations must implement controls, checkpoints, and audit procedures to identify and prevent the adverse actions of insider threats.
    - The challenges posed by insider threats require responses that go beyond conventional, reactive cybersecurity measures (Jones, 2024). Integrating multidisciplinary insights from psychology, criminology, organization, and cybersecurity is a promising strategy for effectively identifying and mitigating these complex threats. As the keeper of the bag, Judas Iscariot can collect money, misinform about the status of that money, and help himself as desired. He can commit collusion and take advantage of the situation. In cybersecurity, these factors are significant for establishing a strong control environment (e.g., segregation of duties). No single individual should have excessive privileges or the ability to access various accounts, creating situations in which they can commit fraud, waste, and abuse, and then hide the evidence by exploiting the accounts. A notable recent insider threat to a religious organization involving financial malfeasance is the case of Joseph Meisch, the former business manager of St. Patrick's Church in New Orleans. In September 2020, Meisch was charged with wire fraud after he embezzled more than $329,000 from church accounts. He used church credit cards for personal expenses and transferred church money to his personal bank accounts, abusing the trust the congregation had placed in him. This incident is reminiscent of the betrayal of Judas, in which a trusted member, Meisch, abuses his authority to gain personal advantage at the expense of the church. This incident underscores the fact that insider threats in religious organizations can cause moral and financial damages, paralleling those in secular organizations. Having

well-documented processes and following efficient audit procedures can reduce the risk of collusion.

- In some cases, malicious behaviors are reportable offenses that carry fines, penalties, and a reputational impact that can be financially incalculable. Insider threats make zero-trust architectures a necessity. Disinformation exemplifies how deceit works against governance. Limited privilege is essential to limit the negative consequences, in like manner as Eden's walls safeguard purity. Accountability can involve audit logs and digital forensics that provide traceability and ethical stewardship in cyberspace.

6.1.5. Biblical Narrative 5: Misrepresented Truth

- Text: Proverbs 14:15. "God made mankind upright, but they have gone in search of many schemes."
- Event: Disguising their appearance to seem harmless, the Gibeonites use misinformation and deception to exploit the trust of the Israelites.
- Data Integrity and Misinformation:
  - Cyber Relevance. Misinformation involves false information, and disinformation efforts, including data integrity issues, seem credible but are harmful. These activities use convincing deceptions to induce individuals to comply with threat actors' desires.
  - Data-backed Insight. More than 70% of organizations report having been targeted by misinformation campaigns (World Economic Forum, 2022).
  - Critical Synthesis. The Israelites have a decree to eliminate the inhabitants from the land. Thus, the Gibeonites, who are their neighbors, wear old clothes and carry moldy bread to disguise themselves as travelers rather than inhabitants. The Israelites "believed every word" provided to them by the Gibeonites without scrutiny or divine consultation. Thus, the Gibeonites can trick (or spoof) the Israelites. The Gibeonites' claims represent a layer of their breach strategy. Their deception mirrors the tactics of false prophets, manipulating appearances and words to bypass scrutiny and exploit trust. Just as the Israelites' signs mislead the Israelites, modern cyber threats depend on social engineering and disinformation. The Bible warns against naivety and emphasizes discernment (Proverbs 14:15), a virtue reiterated in cybersecurity procedures such as validation, verification, and threat intelligence. False prophets, threat actors, and attackers in the cyber domain construct narratives of persuasion to exploit vulnerabilities. Matthew 7:15 warns, "Beware of false prophets, which come to you in sheep's clothing, but inwardly they are ravening wolves." Spiritual and digital discernment are thus equally vital to protecting the integrity of communities, whether sacred or virtual. The Bible warns against gullibility and emphasizes discernment and the capacity to evaluate life forces and establish the truth. Likewise, cybersecurity stresses threat intelligence, reputation checks, and validation to guard against misinformation, which can be detrimental depending on the vulnerability being exploited. From insider threats to state-sponsored attackers, misinformation can be used to deceive and act on malicious intent. False appearances and words lead to misguided promises, so exercising sound judgment is essential.

6.1.6. Biblical Narrative 6: The Tree of Knowledge

- Text: Genesis 2:16–17. "And the Lord God commanded the man, 'You are free to eat from any tree in the garden, but you must not eat from the tree of the knowledge of good and evil, for when you eat from it you will certainly die."

- Event: Adam and Eve are deceived into eating from the Tree of Knowledge and receive calamitous consequences.
- Principle of Least Privilege (PoLP):
    - o Cyber Relevance. Overreach leads to systemic failure. Operating based on the PoLP is a safeguarding practice. In Genesis, the injunction against eating from the Tree of Knowledge establishes a boundary for maintaining things in balance. In cybersecurity, the PoLP is an echo of this establishment of a boundary: providing too much access increases threats, permits insider attacks, privilege misuse, and severe security violations.
    - o Data-backed Insight. Eighty percent of breaches can be prevented by proper application of the PoLP (CyberArk, 2023).
    - o Critical Synthesis. The PoLP is an important principle of security according to which users, programs, or systems should only be allowed to access the bare minimum of resources necessary for their purposes. The principle involves minimizing the risk of serious consequences from a security issue by making attacks difficult to achieve and preventing the spread of malware. By granting users and systems the minimum access that they need, organizations can minimize the risk of security intrusions resulting from breached accounts with extensive privileges. In a biblical context, this principle mirrors the restricted access granted in the Garden of Eden. For their own protection, Adam and Eve are instructed not to eat from the Tree of Knowledge (Genesis 2:16–17). They do not have "a need to know" specific information. However, because they are prime targets, they are deceived and give in to the opposition. The breach in the Garden of Eden changes the course of humanity's earthly sustainability and its lifecycle. Limiting access serves as a safeguard against potential transgressions. The PoLP also applies to knowledge-sharing since information can be used maliciously. Judges 16:4–21 describes how Delilah uses social engineering tactics (trust and questioning) to discover the secret of Samson's strength (i.e., his hair), ultimately gaining access to critical information and using it to compromise him. Ignoring such boundaries as the PoLP can lead to dire consequences. This story illustrates the importance of adhering to defined limits to maintain integrity and security. By connecting modern cybersecurity measures with timeless biblical principles, organizations can cultivate a culture of awareness and moral obligation.

6.1.7. Biblical Narrative 7: Review of Decisions and Actions

- Text: Revelation 20:12. "...and books were opened. Another book was opened, which is the Book of Life.... The dead were judged according to what they had done as recorded in the books."
- Event: The final review of choices and actions in alignment with divine standards.
- Audit and Accountability:
    - o Cyber Relevance. Revelation 20:12 reflects the cybersecurity principle of auditability and traceability, as systems log and examine activities for justice and accountability. Since no act is invisible to divine judgment, no privileged act in secure systems needs to be unrecorded or non-auditable. Record-keeping must be maintained through audit logs backed by immutable records.
    - o Data-backed Insight. 279 companies (8%) revealed material deficiencies in their 2023/2024 annual reports out of 3502 total. Lack of documentation, rules, and processes; accounting resources or knowledge; IT/software/access concerns; segregation of duties/design controls; and insufficient disclosure controls were the top five problems causing major weaknesses.

This indicates that one of the main underlying causes of material weaknesses, which are significant accountability issues, is insufficient documentation (i.e., poor record-keeping/audit trails) (The Corporate Counsel, 2025).

- Critical Synthesis. Divine inquiry models ethical accountability in that all actions are traceable before God. Accordingly, there will come a time when acts performed are assessed for their integrity. Revelation 20:12 speaks of a final judgment according to a perfect record called the Book of Life. Modern cybersecurity controls utilize secure and immutable audit trails so that all actions are accounted for and traceable. This theme recurs in blockchain technology, zero-trust networks, and forensic logging in cybersecurity, where systems that do not forget maintaining accountability and trust. Transparency and accurate records are essential in domains to ensure that intent and action align and that repercussions follow from substantiated behavior, not just the appearance of implications. The Book of Life illustrates perfect traceability, being analogous to the need for tamper-proof logs that hold users and systems accountable for actions taken under their identities. In the domains of religion and the internet alike, genuine justice hinges on what is recorded rather than what is stated. The Book of Life exhibits impeccable tracking, as evidenced by the use of irreversible records that hold individuals and systems accountable for actions carried out in their name.

6.2. The Biblically Framed Cybersecurity (BFCy) Model

The BFCy Model is fundamentally rooted in scripture, while also drawing conceptually on divine command theory and virtue ethics. These ethical frameworks enhance the model's robustness by establishing a moral foundation. The model reconceptualizes cybersecurity from an embedded, faith- and values-based perspective, thereby enhancing cyber governance and organizational resilience. This foundational framework for safeguarding digital assets merges religious principles with cybersecurity methodologies. It indicates that cybersecurity transcends technical concerns, as it involves adapting to the overarching policies and ethical frameworks that enterprises, their personnel, and the stakeholder community must contemplate. The rapid advancement of technologies makes leaders susceptible to the dangers of adhering to outdated techniques and methodologies, which can cause significant difficulties (Aridi et al., 2024; Burrell, 2018).

The BFCy Model is, then, an innovative methodology that amalgamates biblical tenets with modern cybersecurity approaches to establish a comprehensive framework for digital safeguarding. The paradigm interprets cybersecurity as a spiritual duty by referencing scriptures that emphasize stewardship, honesty, vigilance, justice, and compassion in order to protect data and the dignity, trust, and welfare of the individuals it represents. The repercussions of a cyberattack on a religious institution extend beyond the digital realm, manifesting in tangible impacts on its core principles. Financial theft, whether directly from institutional finances or by members through fraudulent emails, can disrupt operational activities and impede core objectives (Maurer & Nelson, 2021). The BFCy Model shows academic theologians that cybersecurity awareness can be enhanced through a practical and scriptural foundation.

Based on the empirical data provided by the global and regional cybersecurity statistics in Table 1, Figure 1 presents the Biblically Framed Cybersecurity (BFCy) Model. This conceptual framework combines enduring ideas from biblical texts with modern cybersecurity tactics, providing a culturally relevant and ethically sound approach to digital risk management. The BFCy Model underscores the cohesive integration of spiritual values with technological defense systems, seeking to bolster organizational resilience

and community trust. The integration of biblical principles with cybersecurity practices centers on embedding ethical, spiritual, and moral values into the foundational culture of technological defense systems. The BFCy Model emphasizes this fusion as a means to enhance organizational resilience and foster enduring trust within communities.

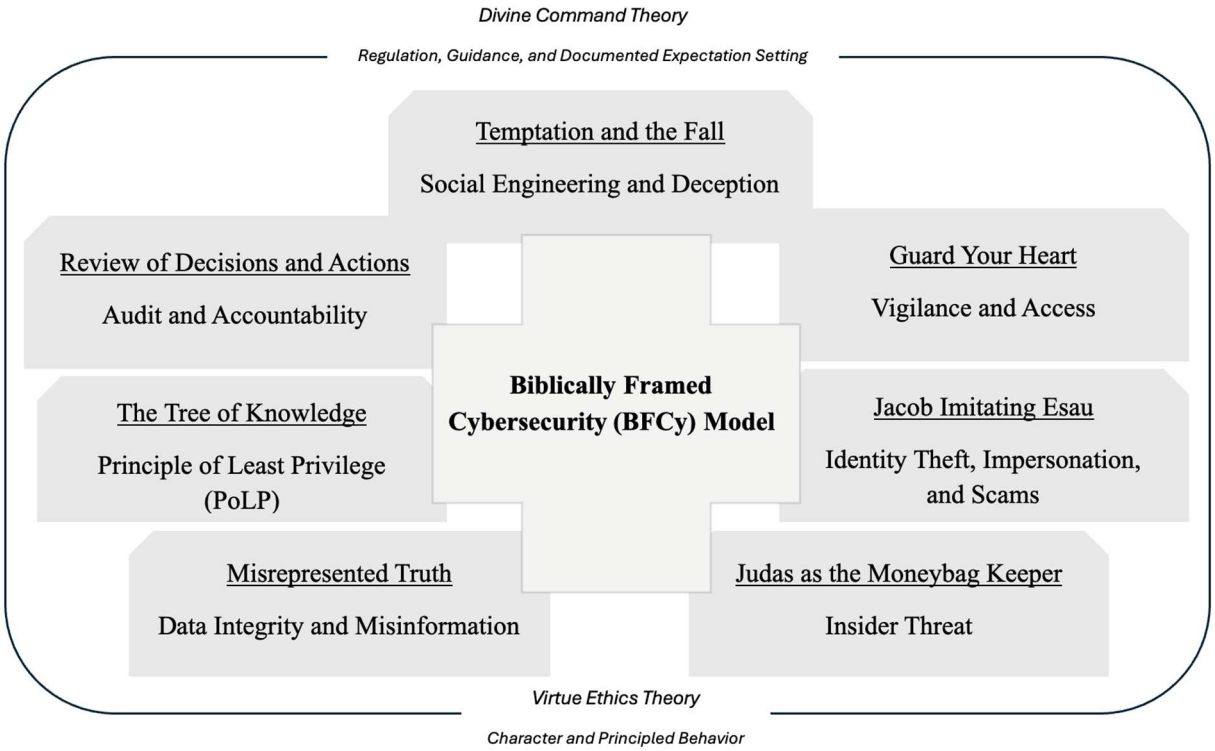

Figure 1. The Biblically Framed Cybersecurity (BFCy) Model. Note. The author of this paper created this figure.

Biblical teachings such as stewardship, vigilance, and integrity are viewed as aligning with essential cybersecurity values. For instance:

- Stewardship is reflected in the responsible management and safeguarding of digital assets and data.
- Vigilance is mirrored in proactive monitoring and defending against threats, echoing biblical admonitions to "watch and pray."
- Integrity shapes policies around confidentiality and honest reporting of vulnerabilities, parallel to scriptural mandates for truthfulness and transparency.

The BFCy Model, while grounded in Christian scripture and ethics, may offer adaptable elements for other faith-based or ethical frameworks. Nonetheless, generalization beyond Christian institutions should be approached with meticulous modification and in collaboration with practitioners or researchers from those traditions. This paper does not assert general applicability and presents the concept mainly as a resource for Christian groups, unless further research or collaborative adaptation provides additional evidence.

The approach integrates scriptural knowledge, behavioral insights, and operational cybersecurity practices, providing a strategic framework for faith-based and mission-driven companies. It promotes a comprehensive concept of cybersecurity that extends beyond just technical solutions, emphasizing stewardship, honesty, vigilance, and community protection as fundamental foundations of effective defense. Figure 1 establishes a vital connection between the statistical reality of cyber threats and the specific contextual requirements of businesses aiming to safeguard their digital assets while upholding their core values. It establishes a foundation for a pragmatic yet insightful examination of cybersecurity

through a biblically informed perspective, cultivating a distinctly strong framework for continuous risk mitigation and ethical governance.

The BFCy Model reconceptualizes regulations and protocols, not as bureaucratic obstacles, but as moral imperatives derived from biblical teachings, thereby highlighting the tangible repercussions of inadequate implementation. Businesses that follow this approach acknowledge that comprehending cutting-edge technology is beneficial, but that ethics and wisdom must guide its use to prevent misuse, exploitation, and harm. Thus, the BFCy Model addresses a critical gap in traditional cybersecurity discourse by integrating ethical considerations, collective accountability, and insights from the primary source of truth. It urges leaders to cultivate environments rich in transparency, ethical consciousness, and moral judgment in which security measures are not simply enforced but align with established principles and insights that significantly affect critical cybersecurity domains, including access controls, data utilization, risk tolerance, and organizational trust.

Organizations must integrate cybersecurity best practices to protect sensitive information and mitigate the risk of cyberattacks (Cybersecurity and Infrastructure Security Agency, 2023). Regular audits should be conducted to identify potential ethical and security weaknesses in computer systems. The audits must evaluate compliance with cybersecurity best practices and organizations' religiously grounded ethical standards. Employing frameworks such as the Cybersecurity Framework 2.0 of the National Institute of Standards and Technology (NIST CSF 2.0) (National Institute of Standards and Technology, 2024) enables organizations to monitor and mitigate cybersecurity threats systematically. The BFCy Model demonstrates that accountability and auditability are essential for maintaining strong cybersecurity procedures. Leaders must cultivate an organizational culture that prioritizes responsibility and openness in cybersecurity, one that encompasses candid communication about security policies, incidents, and ethical challenges. Such actions foster trust among stakeholders and enhance an organization's adherence to established norms and expectations.

In theological organizations, leaders can incorporate cybersecurity issues into theological education, thereby equipping future faith leaders to address the digital challenges that their communities will face (Alkhouri, 2024). Alkhouri (2024) urged leaders to create educational programs that integrate technical cybersecurity training with religious ethics and comprehend the potential effects of breaches from a scriptural viewpoint. Leaders should also promote the involvement of religious communities in cybersecurity knowledge and practices (Cybersecurity and Infrastructure Security Agency, 2023). Such engagement includes organizing workshops, talks, and collaborative initiatives to foster ethical digital conduct and shared accountability. Although it is assumed that individuals comprehend the expectations and are aware of appropriate conduct, it is essential to recognize that "knowing is not doing" (Burrell, 2018), for an employee may complete a security awareness assessment but fail to implement the acquired knowledge (Burton et al., 2023; Renaud & Dupuis, 2023; Triplett, 2022; Wightman & Shakhsheer, 2021).

Numerous factors likely contribute to this "action paradox." According to reactance theory, introduced by Jack W. Brehm (1966), when individuals see a loss or imminent loss of their liberties, they are compelled to reclaim them (see also Wicklund, 2024). Consequently, individuals may oppose rules that impose constraints, particularly if they perceive that the rules limit their options or liberty. Cybersecurity researchers have highlighted this issue (Putri & Hovav, 2014; Renaud & Dupuis, 2023). From another perspective, various psychological characteristics, including dissatisfaction, hostility, control concerns, a mindset of disrespect for authority, and traits associated with antisocial and narcissistic personality types, may lead to dangerous behaviors (Moore et al., 2008; Noonan, 2018; Ohu & Jones, 2025a; Renaud & Dupuis, 2023). The member of an organization may experience elevated

stress levels or workloads (D'Arcy et al., 2014; Nobles & Burrell, 2024) or feel apathy regarding an organization's cybersecurity initiatives because of adverse prior experiences (Nobles, 2022).

6.3. Beyond Moral Exhortation

The BFCy Model encourages religious leaders to establish a comprehensive code of ethics that integrates principles such as honesty, stewardship, and justice into their organizations' cybersecurity practices. As churches progressively transition services online and provide livestreamed worship, their digital presence extends significantly beyond the confines of the sanctuary (Kusuma et al., 2022). This transformation not only exposes church IT systems to cyber threats but also creates a distinct vulnerability at the intersection of church and congregant home networks, particularly through Internet of Things (IoT) devices (Kusuma et al., 2022).

More specifically, livestreaming services connect church equipment and networks with the varied and often less secure home environments of congregants. This process may create opportunities for cybercriminals to exploit vulnerabilities at either end of the connection (New Jersey Cybersecurity and Communications Integration Cell, n.d.). Securing digital interfaces is crucial to safeguard sensitive member information, maintain the integrity of worship experiences, and prevent technology-induced disruptions that could erode trust within faith communities (Kusuma et al., 2022; New Jersey Cybersecurity and Communications Integration Cell, n.d.). The expansion of IoT devices from smart cameras to home streaming systems underscores the need for proactive strategies that integrate scriptural principles of vigilance and prudent stewardship with contemporary risk management to protect the church community and individual congregants as they convene in hybrid digital environments.

The BFCy Model grounds cybersecurity in scriptural and ethical principles by emphasizing stewardship, integrity, vigilance, and justice. Center for Internet Security Critical Security Controls (CIS Controls) version 8 is a widely recognized, prioritized collection of best practices for cybersecurity designed to mitigate tangible threats across businesses of varying scales (Center for Internet Security, 2021). Table 3, a crosswalk table, correlates specific scriptural principles from the BFCy Model with relevant CIS Controls v8 (Center for Internet Security, 2021) and practices to demonstrate how biblical ethics underpin essential cybersecurity disciplines.

Table 3. Cross-Mapping the BFCy Model with Relevant CIS Controls.

Scriptural Principle (BFCy)	Biblical Reference	Key CIS Control	Cybersecurity Practice/Intent	Alignment/Explanation
Stewardship & Accountability	Genesis 1:28; Luke 12:48	Secure Configuration, Audit Log Management	Enforce responsible management of resources	Stewardship requires responsible oversight–configuring, auditing, and securing assets.
Watchfulness & Vigilance	Proverbs 4:23; Matthew 26:41	Security Awareness Training, Monitoring, Continuous Vulnerability Management	Ongoing surveillance, training, and improvement	Scripture calls for watchfulness–mirrored by continual monitoring and vigilance against new threats.
Integrity & Honesty	Proverbs 10:9; Ephesians 4:25	Access Control Management, Data Protection	Accurate authentication, honesty in reporting	The call for truthful action supports practices such as maintaining user integrity and sound authentication.

Table 3. *Cont.*

Scriptural Principle (BFCy)	Biblical Reference	Key CIS Control	Cybersecurity Practice/Intent	Alignment/Explanation
Justice & Equitable Protection	Micah 6:8; Exodus 23:6	Data Protection, Incident Response	Fairness in incident response and recovery	Justice is the concept that systems and processes should offer fair protection and address harms promptly and transparently.
Redemption & Recovery	Psalm 51; Luke 15:11–32	Data Recovery, Incident Response Management	Restoring lost data/operations after attacks	Redemption parallels cyber recovery in emphasizing restoration and improvement after a breach.
Trust but Verify	Proverbs 3:5; 1 John 4:1	Account Management, Audit Log Management	Implement least privilege, verify activity	The Bible cautions against placing trust and wisely underpins "trust but verify" controls.
Community & Shared Responsibility	Acts 2:44–47; Romans 12:4–5	Service Provider Management, User Education	Promote shared cyber hygiene, team accountability	Encourages collective vigilance and mutual accountability for the digital environment.

Note. The author of this paper created this table.

6.4. Cross-Mapping the BFCy Model

The systematic cross-mapping of the Biblically Framed Cybersecurity (BFCy) Model with leading technical standards and controls elucidates how scripturally informed practices resonate with contemporary cybersecurity requirements. This integrative analysis reveals substantive thematic and operational convergence between faith-based ethical imperatives and established frameworks. Such frameworks include the Center for Internet Security (CIS) Controls, the NIST CSF 2.0 (National Institute of Standards and Technology, 2024), and ISO 27001:2022 (Adewole, 2024; International Organization for Standardization [ISO], 2022). Through this comparative lens, several key insights emerge:

- The CIS Controls v8 comprises 18 distinct, actionable domains, including Secure Configuration, Access Control, Data Protection, and Security Awareness Training. Each domain corresponds to the practical requirements addressed in technological frameworks and faith-based ethics.
- The BFCy Model interprets activities such as least privilege, perimeter defense, and quick response as contemporary manifestations of the biblical imperatives to safeguard, discern, and restore.
- The BFCy Model and CIS framework highlight the importance of not only technical controls but also the transformation of corporate culture, training, and leadership.
- Other cybersecurity-related standards, such as the NIST's CSF and the International Organization for Standardization's ISO 27001:2022—Information Security, Cybersecurity, and Privacy Protection–Information Security Management Systems–Requirements, align well with the BFCy Model.

While technical controls are essential, a Biblically Framed Cybersecurity (BFCy) approach must combine these safeguards with specific non-technical, ethical, and cultural initiatives. Neither technical nor human-centric measures are adequate in isolation. Aligning the scriptural and moral principles of the BFCy Model with cybersecurity controls can reveal significant collaboration. Faith-based principles not only validate but also actively strengthen the fundamental behaviors, governance, and controls outlined in generally ac-

cepted cybersecurity frameworks (Renaud & Dupuis, 2023). Researchers have argued that religious values such as stewardship, discipline, accountability, and communal oversight can effectively reinforce the behaviors, governance structures, and controls essential to established cybersecurity frameworks (Alkhouri, 2024; Renaud & Dupuis, 2023). From this perspective, faith-based ethics not only aligns with standards such as NIST CSF 2.0 (National Institute of Standards and Technology, 2024) and ISO 27001:2022 (International Organization for Standardization [ISO], 2022) but can also inform various disciplines and essential cybersecurity practices (Renaud & Dupuis, 2023). This is a compelling and inspiring narrative for church communities seeking spiritual and digital fortitude.

6.5. Actionable Insights

Christian worship leaders can enhance their followers' understanding of the critical importance of cybersecurity by drawing on biblical narratives, providing theological depth and practical information that fosters the development of cybersecurity skills. A crucial suggestion for worship leaders is to reconceptualize biblical accounts in terms of contemporary issues, aligning them with discernment and digital stewardship, for example, and likening the protection of digital borders to the safeguarding of the heart (Proverbs 4:23). To deepen congregations' knowledge of cybersecurity, sermons may emphasize that, similar to the expectation for believers to remain vigilant in prayer and moral in behavior, they must also exercise prudence in their online activities and protect their digital communities. Enhancing security awareness and vigilance can further protect religious institutions, particularly those with an online presence, from cyber threats.

Members of the clergy may reference biblical narratives of deception, such as the serpent in the Garden of Eden (Genesis 3) and Judas's betrayal (Matthew 26; Mark 14; Luke 22; John 18), to emphasize the importance of being vigilant against phishing, identity theft, and insider threats. They can enhance cybersecurity by encouraging congregants to exemplify moral clarity, honesty, and accountability in their online interactions. Worship leaders can subtly incorporate cybersecurity issues into prayer points, devotional readings, and multimedia representations that symbolize digital "gates," "armor," and "walls of protection" during theological and philosophical teachings about cybersecurity, thereby reinforcing the parallels with biblical narratives. This approach conveys knowledge by incorporating cybersecurity awareness into the spiritual growth of the religious community and establishing this awareness as a moral and pastoral responsibility.

The Practical BFCy Daily Operations Checklist provided in this section is designed to connect these overarching concepts with everyday implementation. The checklist translates the theological-philosophical framework of the BFCy Model into practical, habitual behaviors for pastors, church leaders, and IT staff by helping organizations to:

- explicitly define cybersecurity as a moral and spiritual obligation,
- incorporate biblical principles into daily technological policies, training, and operations,
- encourage a culture of vigilance, openness, and mutual support,
- enhance resilience against cyber threats, safeguarding digital assets and community confidence (Nobles, 2022),
- facilitate prompt and knowledgeable responses to incidents, incorporating mechanisms for reconciliation and learning after failures.

Implementing the ideas and framework of the Biblically Framed Cybersecurity (BFCy) Model in practice requires a series of pragmatic, daily operational measures. Table 4 presents a detailed checklist intended to assist faith-based and mission-driven companies in integrating the basic values of the BFCy Model into their regular cybersecurity and organizational practices. This checklist provides explicit, practical criteria that connect with scriptural principles and optimal security standards, enabling teams to remain vigilant,

uphold integrity, and cultivate a culture of stewardship and community safeguarding. The proposed solutions enable the amalgamation of spiritual and ethical concerns with modern cyber risk management, guaranteeing that digital resilience is technically robust and mission-driven.

Table 4. Practical BFCy Daily Operations Checklist.

Task/Recommendation	Frequency	Responsible Party	Scriptural/Ethical Foundation
Establish an ethical and spiritual culture of digital stewardship (including regular affirmations and prayers for discernment and protection)	Quarterly, as scheduled	Pastor/Lead Team	1 Corinthians 4:2; James 1:5; Matthew 6:13 (Spiritual Discipline)
Regularly review and update cybersecurity policies to reflect evolving threats and operational needs	Twice yearly	Leadership, IT, Trustees	Proverbs 10:9 (Integrity)
Maintain secure technical controls (strong passwords, multifactor authentication, access audits, timely patching and updates)	Ongoing	IT, System Administrator	Matt 24:43; Luke 16:10; Prov 27:12 (Vigilance, Alerting, Proactiveness)
Conduct routine cybersecurity awareness training for all staff and volunteers	Twice yearly	IT/Internal or External Partner	Proverbs 4:23 (Vigilance)
Test and evaluate incident response plans through simulated exercises	Annually	Leadership, IT	Galatians 6:1 (Restoration)
Actively share and receive relevant cyber threat intelligence within both internal teams and trusted external partners/networks	As needed/ appropriate	Pastor/IT/ Communications	Ecclesiastes 4:9–10 (Community)

Note. The author of this paper created this table.

The comparative analysis of biblical narratives and contemporary cybersecurity threats demonstrates that faith-based organizations face risks not merely as technical challenges, but as profound ethical and spiritual tests that reflect timeless scriptural patterns. By drawing on scriptural stories, such as the Fall, role-based insider threat, impersonation, least privilege, and accountability, organizations can recognize the psychological manipulation, identity fraud, privilege misuse, and lack of vigilance at the root of many breaches. The Biblically Framed Cybersecurity (BFCy) Model synthesizes these lessons, enabling organizations to embed core virtues such as stewardship, honesty, vigilance, and justice in digital practices and governance. This approach creates a culturally relevant and resilient framework that connects statistical risk realities with a moral code, motivating faith-based entities to cultivate proactive defense, transparent accountability, and enduring community trust as essential aspects of their cybersecurity posture.

Table 4 serves as a valuable tool for staff, volunteers, and leadership, facilitating the implementation of the BFCy Model's goal of achieving enduring, values-based cybersecurity excellence daily.

Further, faith-based cybersecurity frameworks, such as the BFCy Model, translate spiritual principles into robust operational practices that reinforce organizational resilience and foster trust.

6.5.1. Establishing an Ethical and Spiritual Culture

A faith-driven environment begins by embedding digital stewardship into daily organizational life, where ethical conduct is paired with regular affirmations and prayers for discernment and protection. This culture shapes decision-making on privacy, responsible resource use, and transparent communication, framing cybersecurity as a spiritual duty to safeguard information and people.

6.5.2. Policy Development and Continuous Improvement

Organizations regularly review and update cybersecurity policies to align with emerging threats and operational realities. Spiritual maturity informs these revisions, ensuring policies embody fairness, compassion, and an unwavering commitment to protecting all members.

6.5.3. Secure Technical Controls

Robust technical safeguards—including strong passwords, multifactor authentication, thorough access audits, and prompt patching—are maintained as acts of stewardship. These measures are grounded in principles of vigilance and accountability, demonstrating a commitment to the safety and confidentiality of digital assets.

6.5.4. Cybersecurity Awareness Training

Routine training for staff and volunteers strengthens communal vigilance and prepares the organization to recognize evolving threats. Program content weaves together technical education and ethical instruction, empowering individuals to act as responsible stewards in digital and physical domains.

6.5.5. Incident Response Plan Evaluation

Faith-based organizations test and refine incident response procedures through simulated exercises, enabling rapid, coordinated reactions to threats. This preparedness—supported by a foundation of trust and collective accountability—minimizes disruption and ensures organizational stability in moments of crisis.

6.5.6. Collaborative Threat Intelligence Sharing

Active sharing and receipt of cyber threat intelligence within internal teams and with trusted external partners is viewed as an extension of ethical and spiritual responsibility. Such collaboration, grounded in principles of mutual aid and transparency, elevates the organization's collective defense posture and extends stewardship beyond institutional boundaries.

These applications of faith-based cybersecurity frameworks transform technical policies into expressions of communal care, ethical stewardship, and resilient organizational culture, ultimately aligning digital defense with spiritual values.

6.5.7. The BFCY Model and Emerging Threats

Today's threat landscape is rapidly evolving, challenging organizations to address risks that are unprecedented in complexity and scale. AI-driven attacks, zero-day exploits, and the dawn of quantum computing each present formidable new obstacles for digital defense. The Biblically Framed Cybersecurity (BFCy) Model's ethical grounding positions it to provide guidance and resilience as organizations confront these emerging threats.

6.5.8. AI-Driven Assaults

The BFCy Model enhances organizational preparedness against AI-driven cyber threats by promoting ongoing vigilance, ethical stewardship, and proactive adaptation in technology deployment. By grounding risk management in spiritual principles like discernment and collective wisdom, leaders are encouraged to implement layered defenses, continuous monitoring, and responsible use policies that anticipate and detect adversarial AI activities. This moral framework urges organizations to foster a culture that values transparency and ethical innovation, making it easier to recognize and mitigate deceptive techniques employed by malicious AI actors, such as deepfakes, automated phishing, and autonomous malware.

6.5.9. Zero-Day Vulnerabilities

Addressing zero-day vulnerabilities within the BFCy framework requires resilience and accountability, aligned with biblical calls for watchfulness and urgent action when facing unforeseen dangers. Organizations are encouraged to practice thorough documentation, frequent system audits, and diligent patch management while cultivating an environment in which reporting and response are valued over concealment. The model's ethical emphasis on truthfulness and trust-building supports rapid organizational communication and collaboration. This ensures that zero-day threats are countered swiftly through transparent escalation and collective remediation, instead of being overlooked or mishandled.

6.5.10. Quantum Computing

Facing the prospective risks posed by quantum computing, the BFCy Model calls for robust stewardship, intergenerational foresight, and innovative defense aligned with scriptural reflection on wisdom and preparedness. Organizations are prompted to invest in quantum-resistant encryption, adaptive security architectures, and long-term strategic planning, guided by a moral commitment to protect data assets far beyond immediate technological cycles. This approach fosters interfaith and interdisciplinary dialogue, encouraging a consistent review of emerging threats and the ethical implications of cryptographic vulnerabilities. It ensures that values like integrity and justice remain at the heart of policy formation and technological advancements.

The Biblically Framed Cybersecurity (BFCy) Model provides a principled foundation for meeting the escalating challenges posed by emerging threats such as AI-driven attacks, zero-day vulnerabilities, and quantum computing. This framework leverages spiritual values like discernment, stewardship, and accountability to promote organizational vigilance, transparent risk management, and innovative defense practices. By grounding cybersecurity strategy in ethical decision-making and long-term foresight, the BFCy Model equips organizations to proactively recognize and address sophisticated digital risks while maintaining integrity, trust, and resilience amid rapidly evolving technological landscapes.

7. Conclusions

This study aimed to provide a researched perspective on and framework for discussions of cyber risk by incorporating biblical and philosophical ethics into cybersecurity discourse. This approach can be beneficial to academic theologians, clergy, and Christian practitioners seeking to align a moral compass with their area of expertise. Divine command theory, a metaethical framework suggesting that actions are morally right if they align with God's will, corresponds to non-cognitive approaches within moral pragmatism (Máhrik & Králik, 2024). Actions are deemed ethically good when they align with God's will, as revealed through scripture or supernatural revelation. This methodology leverages adherence to divine commands as the cornerstone of ethical conduct. The virtue ethics framework emphasizes cultivating moral character and virtues, including courage, temperance, and justice, and is regarded as an extension of moral philosophy (Hauerwas & Pinches, 2022; Russell, 2023).

Christian virtue and ethics prioritize the cultivation of Christ-like attributes and the advancement of moral excellence through spiritual development and the formation of habits (Galatians 5:22–23; 1 Timothy 4:7–8). For Christian professionals in cybersecurity, this approach can enhance the human factors by utilizing biblical principles and thematic coding to develop a theological and ethical framework for decision-making. The current cybersecurity landscape demands conventional and innovative strategies, including collaborative responses that exceed the capabilities of individual entities or organizations (Burton, 2024).

A brief comparison reveals that while the Biblically Framed Cybersecurity (BFCy) Model draws its ethical foundations from Christian scripture, emphasizing stewardship, vigilance, justice, and integrity, many non-Christian ethical frameworks offer conceptually analogous approaches that enrich digital risk management. For example, Islamic ethics centers on justice, trustworthiness, and community stewardship, as expressed in the principles of Sharia and the teachings of the Quran, guiding data protection and collective accountability. Jewish law, grounded in halakhic tradition, prioritizes truth, social responsibility, and the fair use of technology, with strong prohibitions against deception and misuse of information. Secular humanist and philosophical models, such as Kantian ethics and utilitarianism, emphasize autonomy, transparency, and minimizing harm and are often operationalized through universal standards like the NIST Cybersecurity Framework or ISO 27001:2022. By integrating lessons from diverse traditions—whether Christian, Islamic, Jewish, or philosophical—the significance of the BFCy Model is heightened, positioning it as a conceptual bridge that champions moral clarity, values-driven governance, and community trust in cybersecurity regardless of faith or culture.

A novel integration of biblical ethics, philosophical principles, and theory can enhance cybersecurity decision-making. This comprehensive mix of technical training and faith-based ethics can equip future leaders with the necessary spiritual insight and technical proficiency to meet the challenges of cybersecurity. No entity engaged in internet-related activities is immune to cyberattacks (Cybersecurity and Infrastructure Security Agency, 2023; IBM Security, 2023; Jones, 2024). The research presented here highlights the vital role of human agency, values, and accountability in safeguarding digital landscapes by situating cybersecurity within biblical and ethical frameworks. The BFCy framework encourages deep reflection on how Christian principles of justice, stewardship, and human dignity can guide ethical decision-making in technological environments. Accordingly, academic theologians are encouraged to adopt a more cohesive and value-oriented methodology that integrates heavenly wisdom with modern perspectives, thereby fostering trust, resilience, and integrity in the digital realm amid ever-changing digital threats.

While the cyber threat landscape may seem contemporary, several foundational principles of cybersecurity, such as vigilance, moral integrity, and the consequences of immoral actions, resonate deeply with venerable biblical teachings. The parallels are striking; thus, the call to guard the heart (Proverbs 4:23) mirrors the necessity to secure access points. Moreover, the admonitions against deception resonate with the efforts to combat phishing and social engineering. Nevertheless, the rapid flow of threats tends to overshadow the ageless wisdom inherent in scriptural truths.

The Bible emphasizes the value of defending boundaries, the perils of misplaced trust, and the virtues of accountability (e.g., Nehemiah 4:9; Proverbs 4:23). Its teachings align with foundational concepts of cybersecurity, such as least privilege, auditability, and proactive defense. Executives who internalize these teachings can create sustained structures that enhance compliance and foster character by providing security practices rooted in integrity and foresight. Pressing questions include how to integrate enduring biblical principles into managing cyber threats and what can be learned from narratives such as the Fall of Eden (Genesis 3:13), in which unrestricted access and deception resulted in irreparable harm, and the tale of Judas, in which insider betrayal offers a bitter lesson regarding the dangers lurking in trusted spaces. These moral teachings serve as cautionary tales for the contemporary virtual world.

This ethical and comprehensive approach to digital resilience integrates enduring principles with contemporary technological comprehension. Future studies can integrate biblical ethics and cybersecurity by addressing responsibility, insider threats, and disinformation to enhance awareness of the implications and potential of this approach. Further

research is essential to demonstrate how biblical ethics and philosophical frameworks can guide responses to cybersecurity threats. Thus, a qualitative study utilizing semi-structured interviews with religious leaders could investigate the meaningful application of theological–ethical decision frameworks (Buzguta, 2024; Montero Orphanopoulos, 2025), including divine command theory (Máhrik & Králik, 2024) and virtue ethics (Hauerwas & Pinches, 2022; Russell, 2023), to cybersecurity practices. An empirical study or case-based use of the BFCy model could enhance its practical significance, and interviews, case studies, or simulations could validate the model.

Key takeaways indicate that integrating biblical and philosophical ethics, including divine command theory and virtue ethics, into cybersecurity discourse provides a vital moral and spiritual grounding for managing digital risks. This comprehensive framework supports academic theologians, faith leaders, and Christian practitioners in weaving core scriptural values, such as stewardship, justice, and vigilance, into technical practices and leadership decision-making. The research highlights that no entity is exempt from cyber threats and that effective risk management increasingly relies on cultivating moral character, accountability, and collaborative strategies grounded in principled wisdom. Drawing explicit connections between biblical narratives and modern threats enhances the relevance of cybersecurity protocols while also prompting further inquiry into the practical application and validation of faith-informed ethical models in real-world organizational settings. This holistic approach not only strengthens digital resilience but also encourages ongoing research and dialogue to adapt ancient ethical insights to the evolving landscape of cyber risk.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing does not apply to this manuscript.

Acknowledgments: The author gives thanks to God for His inspiration, direction, and grace in completing this research.

Conflicts of Interest: The author declares no conflict of interest.

References

Adewole, S. A. (2024). *Security and salvation: Exploring the unexpected parallels between cybersecurity and Christianity*. Digital Security Insights. Available online: https://www.linkedin.com/pulse/security-salvation-exploring-unexpected-parallels-between-adewole-jrpzf/ (accessed on 24 April 2025).

Alkhouri, K. I. (2024). Exploring the interplay of cybersecurity practices and religious psychological beliefs in the digital age. *Theophany*, *6*, 25–52. [CrossRef]

Aridi, A. S., Burrell, D. N., Finch, A., Burton, S. L., Quisenberry, W. L., Jones, L. A., Daryousef, M., Graf, D. G., Espinoza, M. D., & Mondala-Duncan, M. (2024). Coaching cybersecurity project managers and cybersecurity engineers. In *Evolution of cross-sector cyber intelligent markets* (pp. 356–377). IGI Global Scientific Publishing. [CrossRef]

Bandura, A. (1990). Selective activation and disengagement of moral control. *Journal of Social Issues*, *46*(1), 27–46. [CrossRef]

Brehm, J. W. (1966). *A theory of psychological reactance*. Academic Press.

Buller, D. B., & Burgoon, J. K. (1996). Interpersonal deception theory. *Communication Theory*, *6*(3), 203–242. [CrossRef]

Burrell, D. N. (2018). An exploration of the critical need for formal training in leadership for cybersecurity and technology management professionals. *International Journal of Hyperconnectivity and the Internet of Things*, *2*(1), 52–67. [CrossRef]

Burton, S. L. (2024). Cross-sector collaboration and information sharing: Intelligent cybersecurity markets. In *Leadership action and intervention in health, business, education, and technology* (pp. 197–221). IGI Global. [CrossRef]

Burton, S. L. (2025). Digital saboteurs: Unmasking insider cybersecurity threats in aviation and aerospace. *Law, Economics and Society*, *1*(2), 1. [CrossRef]

Burton, S. L., Burrell, D. N., & Nobles, C. (2023). Adapting to the cyber-driven workforce: A battle for the discouraged worker. In *Real-world solutions for diversity, strategic change, and organizational development: Perspectives in healthcare, education, business, and technology* (pp. 130–152). IGI Global. [CrossRef]

Burton, S. L., & Moore, P. D. (2024). Pig butchering in cybersecurity: A modern social engineering threat. *SocioEconomic Challenges*, *8*(3), 46. [CrossRef]

Buzguța, C. B. (2024). The morality of Christian love: A theological and ethical perspective. *Scientia Moralitas: International Journal of Multidisciplinary Research*, *9*(2), 53–64. Available online: https://www.scientiamoralitas.com/index.php/sm/article/view/289 (accessed on 16 July 2025).

Center for Internet Security. (2021). *CIS critical security controls version 8*. Available online: https://www.cisecurity.org/controls/cis-controls-list (accessed on 17 July 2025).

CyberArk. (2023). *CyberArk 2023 identity security threat landscape report*. Available online: https://www.cyberark.com/resources/ebooks/cyberark-2023-identity-security-threat-landscape-report (accessed on 28 May 2025).

Cyber Command. (n.d.). *Understanding cybersecurity risks for nonprofits: The ultimate guide*. Available online: https://cybercommand.com/cybersecurity-risk-for-nonprofit (accessed on 28 May 2025).

CyberPeace Institute. (2023, December 7). *NGOs serving humanity at risk: Cyber threats affecting "International Geneva"*. CyberPeace Analytical Report. Available online: https://cyberpeaceinstitute.org/publications/cyberpeace-analytical-reportngos-serving-humanity-at-risk-cyber-threats-affecting-international-geneva/ (accessed on 7 July 2025).

CyberPeace Institute. (2024, March 25). *Cyber poor, target rich: The crucial role of cybersecurity in nonprofit organizations*. Available online: https://cyberpeaceinstitute.org/news/cyber-poor-target-rich-the-crucial-role-of-cybersecurity-in-nonprofit-organizations (accessed on 7 July 2025).

Cybersecurity and Infrastructure Security Agency. (2023). *Mitigating attacks on houses of worship security guide*. U.S. Department of Homeland Security. Available online: https://www.cisa.gov/resources-tools/resources/mitigating-attacks-houses-worship-security-guide (accessed on 17 June 2025).

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285–318. [CrossRef]

D'Cruz, P., Du, S., Noronha, E., Praveen Parboteeah, K., Trittin-Ulbrich, H., & Whelan, G. (2022). Technology, megatrends and work: Thoughts on the future of business ethics. *Journal of Business Ethics*, *180*, 879–902. [CrossRef]

Department for Science, Innovation and Technology. (2025). *Cyber security breaches survey 2025*. U.K. Government. Available online: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025 (accessed on 19 June 2025).

Drucker, P. F. (1981). What is business ethics? *The Public Interest*, *63*, 18–36.

Firch, J. (2025, May 24). *The average cost of ransomware attacks* (Updated 2025). Purplesec. Available online: https://purplesec.us/learn/average-cost-of-ransomware-attacks/ (accessed on 28 May 2025).

Gryder, M. (2025, July 9). *FB-ISAO threat level statement update, 09 July 2025—Threat levels remain at elevated*. FB-ISAO. Available online: https://faithbased-isao.org/faith-based-daily-awareness-post-10-july-2025/ (accessed on 21 July 2025).

Hadlington, L. (2018). The "human factor" in cybersecurity: Exploring the accidental insider. In J. McAlaney, L. A. Frumkin, & V. Benson (Eds.), *Psychological and behavioral examinations in cyber security* (pp. 46–63). IGI Global. [CrossRef]

Harvard Business Review. (2023, May 4). *The devastating business impacts of a cyber breach*. Available online: https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach (accessed on 19 June 2025).

Hauerwas, S., & Pinches, C. (2022). *Christians among the virtues: Theological conversations with ancient and modern ethics*. University of Notre Dame Press.

Hoffman, W. M., & Moore, J. M. (1982). What is business ethics? A reply to Peter Drucker. *Journal of Business Ethics*, *1*(4), 293–300. [CrossRef]

IBM Security. (2023, July 24). *Cost of a data breach report 2023*. Available online: https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs (accessed on 19 June 2025).

Identity Defined Security Alliance. (2023). *2023 trends in securing digital identities*. Available online: https://www.idsalliance.org/research/ (accessed on 7 June 2025).

International Committee of the Red Cross. (2022, January 19). *Cyber-attack on ICRC: What we know*. Available online: https://www.icrc.org/en/document/sophisticated-cyber-attack-targets-red-cross-red-crescent-data-500000-people (accessed on 12 May 2025).

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection—Information security management systems—Requirements* (ISO/IEC 27001:2022). ISO. Available online: https://www.iso.org/standard/82875.html (accessed on 4 May 2023).

Jones, L. A. (2021). A content analysis review of literature to create a useable framework for reputation risk management. In *Handbook of research on multidisciplinary perspectives on managerial and leadership psychology* (pp. 91–133). IGI Global. [CrossRef]

Jones, L. A. (2024). Unveiling human factors: Aligning facets of cybersecurity leadership, insider threats, and arsonist attributes to reduce cyber risk. *SocioEconomic Challenges*, *8*(2), 44–63. [CrossRef]

Jones, L. A., & Burrell, D. N. (2025). Illegal cybersecurity threats created by organizational arsonists in healthcare organizations. *Law, Economics and Society*, *1*(1), 93. [CrossRef]

Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk prediction for the critical infrastructure protection. *Neural Computing and Applications*, *34*(18), 15241–15271. [CrossRef]

Kusuma, S. D., Saputra, S., Sugianto, E., & Parinussa, S. (2022, July). Using the Internet of Things to improve Christian ministry in the present era. In *International conference on theology, humanities, and christian education (ICONTHCE 2021)* (pp. 218–220). Atlantis Press. [CrossRef]

Maurer, T., & Nelson, A. (2021). *The global cyber threat*. International Monetary Fund. Available online: https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm (accessed on 9 May 2025).

Máhrik, T., & Králik, R. (2024). Divine command theory–Potentiality and limits. *Journal of Education, Culture and Society*, *15*(1), 19–28. [CrossRef]

Mimecast. (2025). *State of human risk 2025*. Mimecast Limited. Available online: https://www.mimecast.com/resources/ebooks/state-of-human-risk-2025/ (accessed on 14 June 2025).

Montero Orphanopoulos, C. (2025). Fundamental theological ethics "in exit": New categories and interdisciplinary approaches to human social flourishing. *Religions*, *16*(4), 448. [CrossRef]

Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. (2008). The "big picture" of insider IT sabotage across US critical infrastructures. In S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, S. W. Smith, & S. Sinclair (Eds.), *Insider attack and cyber security. Advances in information security* (Vol. 39, pp. 17–52). Springer. [CrossRef]

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST Cybersecurity White Paper No. NIST.CSWP.29). U.S. Department of Commerce. [CrossRef]

New International Version. (2011). *The holy bible*. Zondervan. Available online: www.biblegateway.com/versions/New-International-Version-NIV-Bible/ (accessed on 11 April 2025).

New Jersey Cybersecurity and Communications Integration Cell. (n.d.). *IoT device security and privacy*. Available online: https://www.cyber.nj.gov/guidance-and-best-practices/device-security/iot-device-security-and-privacy (accessed on 30 May 2025).

Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *Holistica Journal of Business and Public Administration*, *13*(1), 49–72. [CrossRef]

Nobles, C., & Burrell, D. (2024). Exploring the variability of human factors definitions in cybersecurity literature. *MWAIS 2024 Proceedings*, 28. Available online: https://aisel.aisnet.org/mwais2024/28 (accessed on 22 June 2025).

Noonan, C. F. (2018). *Spy the lie: Detecting malicious insiders*. U.S. Department of Energy. Available online: https://irp.fas.org/eprint/noonan.pdf (accessed on 11 May 2025).

Office of Intelligence and Analysis. (2025). *Homeland threat assessment*. U.S. Department of Homeland Security. Available online: https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf (accessed on 17 June 2025).

Ohu, F. C., & Jones, L. A. (2025a). An examination of digital validation-seeking behaviors in adolescents as precursors to romance scamming. *Scientia Moralitas*, 10. Available online: https://scientiamoralitas.education/wp-content/uploads/2025/04/Scientia-Moralitas-Conference-Proceedings5.pdf (accessed on 11 July 2025).

Ohu, F. C., & Jones, L. A. (2025b). Validation syndrome: The root of deception and developmental predictors of dark triad traits in adolescents for forensic and developmental psychology. *International Educational Research*, *8*(2), 67. [CrossRef]

Pattison-Gordon, J. (2022, November 15). *"Data-rich, resources-poor": CIS report targets gaps in K-12 cyber*. Government Technology. Available online: https://www.govtech.com/security/data-rich-resources-poor-cis-report-targets-gaps-in-k-12-cyber (accessed on 6 May 2025).

Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. *International Journal on Soft Computing*, *14*(3), 1–16. [CrossRef]

Petrosyan, A. (2022). *Annual cybersecurity and cyber insurance spending worldwide from 2015 to 2020*. Statista. Available online: https://www.statista.com/statistics/387868/it-cyber-securiy-budget/ (accessed on 6 June 2025).

Petrosyan, A. (2023). *Annual cost of cybercrime worldwide 2017–2028*. Statista. Available online: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide (accessed on 8 July 2025).

Ponemon Institute. (2023). *Cost of insider risks global report-2023*. Available online: https://ponemonsullivanreport.com/2023/10/cost-of-insider-risks-global-report-2023 (accessed on 6 May 2025).

Putri, F. F., & Hovav, A. (2014, June 9–11). *Employees' compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory*. European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel. Available online: http://aisel.aisnet.org/ecis2014/proceedings/track16/2 (accessed on 15 June 2025).

Renaud, K., & Dupuis, M. (2023). Cybersecurity insights gleaned from world religions. *Computers & Security*, *132*, 103326. [CrossRef]

Reuters. (2025). *FBI says cybercrime costs rose to at least $16 billion in 2024*. Available online: https://www.reuters.com/world/us/fbi-says-cybercrime-costs-rose-least-16-billion-2024-2025-04-23/? (accessed on 30 June 2025).

Roberts, R. (2023). *Cybercrime and religious institutions: A wake-up call for the faithful*. Carr, Riggs, & Ingram. Available online: https://www.criadv.com/insight/cybercrime-and-religious-institutions-a-wake-up-call-for-the-faithful/? (accessed on 15 June 2025).

Roering, R. (2014, September 18). *Keeping your customers and recovering your reputation after a data breach*. Forbes. Available online: https://www.forbes.com/sites/symantec/2014/09/18/keeping-your-customers-and-recovering-your-reputation-after-a-data-breach/ (accessed on 15 June 2025).

Russell, C. (2023). Virtue ethics. In A. Farazmand (Ed.), *Global encyclopedia of public administration, public policy, and governance* (pp. 13255–13260). Springer International Publishing. [CrossRef]

Saeed, S., Jhanjhi, N. Z., Khan, M. A., & Yadav, D. K. (2025). Digital transformation and cybersecurity challenges. *Frontiers in Computer Science*, *7*, 1631362. [CrossRef]

Schoorman, F. D., Mayer, R. C., & Davis, J. H. (1996). Organizational trust: Philosophical perspectives and conceptual definitions. *Academy of Management Review*, *21*(2), 337–340. [CrossRef]

SC Media. (2024, October 7). *Cyberattacks hit religious organizations*. Available online: https://www.scworld.com/brief/cyberattacks-hit-religious-organizations (accessed on 12 May 2025).

Shadbad, F. N. (2021). *Understanding employee non-malicious intentional and unintentional information security misbehaviors* [Unpublished doctoral dissertation]. Oklahoma State University.

Smith, G. (2016). The dramaturgical legacy of Erving Goffman. In *The drama of social life* (pp. 57–72). Routledge.

The Church of Jesus Christ of Latter-day Saints. (2022). *Statement and FAQ on church account data incident*. Newsroom. Available online: https://www.churchofjesuschrist.org/?lang=eng (accessed on 12 May 2025).

The Corporate Counsel. (2025). *Internal controls: Takeaways from 5 years of data on material weaknesses*. The CorporateCounsel.net. Available online: https://www.thecorporatecounsel.net/blog/2025/04/internal-controls-takeaways-from-5-years-of-data-on-material-weaknesses.html (accessed on 30 July 2025).

Thomas, B. Y., & Biros, D. P. (2020). An empirical evaluation of interpersonal deception theory in a real-world, high-stakes environment. *Journal of Criminal Psychology*, *10*(3), 185–199. [CrossRef]

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, *2*(3), 573–586. [CrossRef]

Troilo, G., De Luca, L. M., & Guenzi, P. (2017). Linking data–rich environments with service innovation in incumbent firms: A conceptual framework and research propositions. *Journal of Product Innovation Management*, *34*(5), 617–639. [CrossRef]

Verizon. (2023). *2023 data breach investigations report*. Verizon Communications Inc. Available online: https://www.verizon.com/business/resources/reports/dbir/ (accessed on 12 May 2025).

Wicklund, R. A. (2024). *Freedom and reactance*. Routledge.

Wightman, S. C., & Shakhsheer, B. A. (2021). Informed decision-making: Knowing is not the same as doing. *Journal of the American College of Surgeons*, *233*(4), 578–579. [CrossRef]

World Economic Forum. (2022). *Global cybersecurity outlook 2022*. Available online: https://www.weforum.org/reports/global-cybersecurity-outlook-2022 (accessed on 12 May 2025).