The Vatican needs a CISO office

Foreword: A Digital Call to Protect the Holy See in the 21st Century

The Holy See, the spiritual nucleus for over a billion souls and a sovereign entity with global diplomatic reach, stands at a unique crossroads. An institution rooted in millennia of tradition, it now navigates an increasingly complex digital world. Its mission, unchanged through ages, today relies significantly on digital platforms, communication networks, and data. This digital transformation, while offering unprecedented opportunities for evangelization, administration, and the preservation of its immense cultural heritage, also exposes the Vatican to a new frontier of threats – sophisticated, persistent, and capable of inflicting profound damage.

As the initiator of the Vatican CyberVolunteers, a group of dedicated cybersecurity professionals who have worked since 2022 to provide a measure of digital defense to the Holy See [1], this author has witnessed firsthand the escalating nature of these threats. The CyberVolunteers, likened to a "digital Swiss Guard" [1], have strived to share threat intelligence, identify vulnerabilities through penetration testing, and offer support where possible.[1] However, such voluntary, and often reactive, efforts, while born of sincere dedication, cannot substitute for a formal, strategic, and empowered cybersecurity leadership structure. The very existence of such a group, performing core security functions for a sovereign state, underscores a critical lacuna in the official, resourced capabilities necessary to protect an institution of such global significance. The goal of the CyberVolunteers has always been to "wake them up because they are constantly under attack" [1], highlighting the urgent need for a paradigm shift in the Vatican's approach to cybersecurity.

This article posits that the establishment of a dedicated Chief Information Security Officer (CISO) office within the Vatican is not merely an advisable upgrade but an existential necessity. It is a call to action, rooted in direct experience and a deep-seated desire to protect the Holy See’s invaluable assets, its global mission, and its unique place in the world. The "digital Swiss Guard" analogy, while evocative, points to a far more comprehensive need than can be met by volunteers alone; it points to the need for strategic command, policy, and enterprise-wide governance – functions that are the hallmark of a CISO. This analysis will demonstrate, through factual evidence and rigorous reasoning, why such an office is indispensable for safeguarding the Vatican's digital dominion in the 21st century and beyond.

Joseph Shenouda

I. The Vatican's Expanding Digital Dominion: Treasures and Vulnerabilities in a Connected World

The Holy See and Vatican City State are no longer mere observers of the digital age; they are active participants, increasingly reliant on a complex digital infrastructure to fulfill their diverse missions. This digital expansion, while vital, simultaneously broadens the attack surface and elevates the stakes for information security.

A. The Holy See's Growing Reliance on Digital Infrastructure

The Vatican's digital footprint is vast and multifaceted. It encompasses global communication networks essential for the Church's worldwide administration and pastoral care. An extensive online presence is maintained through a multitude of official websites for Dicasteries, institutions, services, and news dissemination, such as vatican.va, vaticannews.va, and numerous others connected to specific Church bodies.[2] The Dicastery for Communication, for instance, oversees this entire communications network, tasked with unifying the Holy See's communication activities and leveraging "technological innovations and forms of communication currently available".[4]

Beyond public-facing platforms, digital systems are integral to the internal operations of Vatican City State. These support functions ranging from healthcare and economic management to the administration of the world-renowned Vatican Museums.[6] The Directorate of Telecommunications and Information Systems is a cornerstone of this infrastructure, providing core services such as an Internet Service Provider and managing information systems for the State and Holy See bodies.[6]

Furthermore, the Vatican is actively adopting advanced technologies. A notable example is the creation of a "digital twin" of St. Peter's Basilica, a virtual 3D replica generated from 26,000 files and over three terabytes of data, hosted on a cloud platform. This project, aimed at preserving the iconic basilica, involves sophisticated laser scanning, photogrammetry, and IoT sensor integration for remote monitoring and maintenance.[7] This highlights not only the use of cutting-edge technology but also the creation and management of massive, invaluable digital assets.

The Holy See is also proactively engaging with artificial intelligence. Recently enacted AI guidelines demonstrate a commitment to integrating AI ethically into various domains, including governance, judicial processes, administrative functions, and cultural heritage preservation.[8] These guidelines underscore the Vatican's intent to harness AI's potential while upholding human dignity and the common good, but also signify a deeper integration of complex data processing and digital dependencies into its core activities.

B. An Inventory of Irreplaceable Digital and Digitized Assets

The value of the Vatican's digital and digitized assets is, quite simply, incalculable. These are not merely records; they are the historical memory of the Catholic Church, testaments to centuries of human faith and endeavor, and critical instruments of contemporary governance and diplomacy.

At the forefront are the contents of the Vatican Apostolic Archive (formerly the Vatican Secret Archive) and the Vatican Apostolic Library. These institutions house centuries of papal records, state papers, diplomatic correspondence, account books, and theological treatises.[11] The Archive alone is estimated to contain 85 kilometers of shelving.[11] Significant digitization efforts are underway; by 2018, the Archive reported 180 terabytes of digital storage capacity with over seven million images digitized [11], and the Library has made tens of thousands of manuscripts accessible online via platforms like DigiVatLib, even exploring Web3 and NFT technologies for preservation and access with partners like NTT DATA.[13] These initiatives create new digital assets of immense historical and cultural importance.

Diplomatic communications represent another category of highly sensitive digital assets. The Secretariat of State, responsible for the political and diplomatic functions of the Holy See [14], relies on secure digital channels for its global interactions. Historical diplomatic files, such as the Myron C. Taylor papers detailing WWII-era relations [15], illustrate the nature of the sensitive information that is increasingly born-digital or digitized.

Financial and administrative records are also critical. Entities like the Supervisory and Financial Information Authority (ASIF) manage sensitive financial data, including suspicious activity reports (SARs), as part of the Vatican's efforts to ensure financial transparency and combat illicit activities.[16] Various economic directorates and internal administrative systems across Vatican City State also process and store vital operational data.[6]

Personal data constitutes a significant and sensitive component of the Vatican's digital holdings. This includes information on clergy, Vatican employees, and potentially millions of faithful who interact with Vatican services, participate in Church processes, or whose data is processed for pastoral or administrative purposes. The Vatican's own AI guidelines recognize the profound importance of protecting personal and biometric data, underscoring the ethical and security obligations involved.[8]

Finally, cultural heritage data extends beyond the Archives and Library to include digital information from the Vatican Museums [6], the aforementioned digital twin of St. Peter's Basilica [7], and other digitized artifacts. These assets are not just data points; they represent spiritual, cultural, historical, and diplomatic capital of global significance. Their compromise could lead to consequences far exceeding typical data breaches, potentially causing diplomatic incidents, eroding trust, enabling the manipulation of historical narratives, or undermining the Church's spiritual authority. The risk calculus for the Vatican concerning its digital assets must therefore be fundamentally different and more profound than for standard organizations, demanding an exceptionally high level of protection.

C. Current IT Governance and Nascent Security Initiatives

The Vatican is not without IT governance structures or security initiatives. The Directorate of Telecommunications and Information Systems, established in 2008, is responsible for computer networks, related programs, maintenance, and guaranteeing communications and data security. Notably, this Directorate includes a Computer Emergency Response Team (CERT).[6] However, the specific strategic mandate, resources, and operational capabilities of this CERT beyond its mere existence are not publicly detailed, raising questions about its capacity to address the full spectrum of modern cyber threats proactively.[6]

The Directorate of Security and Civil Protection Services, headed by Gianluca Gauzzi Broccoletti—an individual with a background in cybersecurity dating back to his 1999 responsibility for designing Vatican networking technology and cybersecurity infrastructure [18]—plays a role in both physical and, increasingly, cyber protection. This is particularly evident during sensitive events such as papal conclaves, where measures like signal jammers and sweeps for unauthorized devices are employed to ensure secrecy and integrity.[19]

The recently introduced AI Guidelines have led to the planned formation of an AI Commission. This commission will include members from the Directorate of Telecommunications and Information Systems and the Directorate of Security and Civil Protection Services, indicating a degree of cross-departmental collaboration on the governance of specific advanced technologies.[8] Furthermore, the Dicastery for Communication has a significant role in managing the Holy See's overall communication network and its institutional website, vatican.va.[4]

Despite these individual entities and initiatives, a critical gap persists: the absence of an overarching, C-level strategic information security leader—a Chief Information Security Officer (CISO)—responsible for the *entirety* of the Holy See and Vatican City

State's digital assets and comprehensive cyber risk posture. Current efforts, while valuable in their respective domains, appear siloed or event-driven. The Vatican's rapid digital expansion, evidenced by projects like the St. Peter's digital twin and the adoption of AI, seems to be outpacing the maturation of its centralized, strategic cybersecurity governance. While there is foresight in specific technological applications and their ethical considerations, this has not yet translated into a holistic, proactive cybersecurity posture that comprehensively secures the *use* of technology across the entire institution. This suggests a potential cultural or structural lag in recognizing cybersecurity as a fundamental enabler and protector of all digital initiatives, rather than an isolated IT concern or a security measure reserved for high-stakes events.

II. The Unseen Siege: Escalating Cyber Threats Targeting the Heart of Global Faith

The Vatican's expanding digital dominion exists within a perilous global cyber threat landscape. Far from being immune, the Holy See is a high-value target, subject to a range of documented attacks and facing an alarming increase in malicious activity. Objective international benchmarks further underscore the critical vulnerabilities that must be urgently addressed.

A. The Stark Reality: Documented Cyberattacks and Rising Threats

The threats facing the Vatican are not theoretical; they are tangible and have already manifested in significant security incidents.

One of the most prominent examples is the state-sponsored attack attributed to the group "RedDelta," reportedly linked to the Chinese state. In 2020, RedDelta targeted mail servers belonging to the Vatican and the Catholic Diocese of Hong Kong.[1] This campaign occurred during sensitive negotiations between the Vatican and China regarding the appointment of bishops.[1] The attackers employed sophisticated methods, including spear-phishing emails containing customized PlugX malware, with the apparent objectives of gaining insight into the Holy See's negotiating position and monitoring the Hong Kong diocese's stance on pro-democracy movements.[22] This incident clearly demonstrates the Vatican's vulnerability to advanced persistent threats (APTs) with geopolitical motivations.

More recently, in November 2022, several official Vatican websites, including vatican.va, went dark for hours.[1] This disruption occurred a day after Pope Francis made strong criticisms regarding Russia's invasion of Ukraine.[1] While the exact cause was not definitively stated as a cyberattack by official Vatican sources, it was attributed to an "abnormal number of interactions with the site" and "maintenance" or "ordinary maintenance work" by some, and a suspected hack or Distributed Denial of Service (DDoS) attack by others.[23] The timing raised strong suspicions of a retaliatory cyber action.

The Vatican CyberVolunteers have provided further alarming data. In the 12 months leading up to May 2025, the group reported a 150% increase in attacks targeting the Holy See.[1] Their findings include attempts to "phish" or compromise cardinals' online accounts, DDoS attacks aimed at forcing websites offline, and even the discovery of malicious Wi-Fi transmitters placed within and near Vatican City to trick staff into divulging credentials or allowing hackers into systems.[1] Based on their observations, the CyberVolunteers assessed the threat level as "orange" on the Alert Level Information system, indicating a high risk of activity targeting or compromising core infrastructure.[1]

B. An Objective Assessment: International Cybersecurity Benchmarks

External, objective assessments of the Vatican's cybersecurity posture paint a stark and concerning picture, corroborating the urgent warnings from volunteer defenders.

The International Telecommunication Union (ITU), a United Nations agency, in its fifth Global Cybersecurity Index (GCI) for 2024, listed Vatican City State in Tier 5 – the lowest possible performance category. This places the Vatican alongside nations such as Afghanistan, the Maldives, and Yemen in terms of cybersecurity preparedness.[1] Most damningly, the report indicated that on technical cybersecurity measures, the Vatican scored a flat zero out of a possible 20 points.[1]

Further detailed deficiencies are highlighted by the National Cyber Security Index (NCSI), managed by the e-Governance Academy in Estonia. According to 2022 data (reported March 2023), Vatican City State received zero scores across a multitude of critical cybersecurity indicators.[26] These include:

- **No dedicated cybersecurity policy unit:** Lack of a central government entity responsible for national cybersecurity policy development.
- **No formal cybersecurity policy coordination format:** Absence of a committee or working group for national-level coordination.
- **No national cybersecurity strategy or implementation plan.**
- **No cyber threat analysis unit:** Lack of a specialized unit for national strategic cyber threat analysis.
- **No formal national-level cyber incident response unit (CSIRT/CERT):** While the Directorate of Telecommunications lists a CERT, the NCSI indicates no

formally recognized national-level unit meeting its criteria for incident detection and response.

- **No overarching personal data protection legislation** and no independent data protection authority.

The NCSI did register minimal positive scores for "representation in international cooperation formats" (specifically mentioning ITU-Impact) and for the fact that "cybercrimes are criminalized" under Vatican law.[26] However, these minor points are overshadowed by the profound gaps in foundational cybersecurity governance, strategy, and operational capabilities.

The following table provides a snapshot of the Vatican's cybersecurity posture based on these international benchmarks, illustrating the extent of the identified deficiencies:

Table 1: Vatican City State Cybersecurity Posture: An International Comparative Snapshot

NCSI Indicator Category	Specific NCSI Indicator (2022 Data)	Vatican City Score/Status	ITU GCI Technical Score (2024)	Implication of Deficiency
Cybersecurity Policy Development	Cyber security policy unit	0/3 (Not established)	0/20 (Overall Technical Measures)	Lack of central leadership and direction for cybersecurity.
	Cyber security policy coordination format	0/2 (Not established)		Inability to coordinate cybersecurity efforts across different Vatican entities.
	Cyber security strategy	0/1 (Not established)		Absence of a strategic roadmap for managing cyber risks and building resilience.

	Cyber security strategy implementation plan	0/1 (Not established)		No actionable plan to execute any potential strategic cybersecurity goals.
Cyber Threat Analysis & Information	Cyber threats analysis unit	0/3 (Not established)		Limited capacity to understand, analyze, and anticipate cyber threats.
	Public cyber threat reports published	0/1 (Not established)		Lack of transparency and information sharing about the threat landscape.
Incident & Crisis Management	Cyber incidents response unit (CSIRT/CERT)	0/3 (Not established)		No recognized national-level capability to effectively detect and respond to incidents.
	Reporting responsibility for incidents	0/1 (Not established)		Critical incidents may go unreported or uncoordinated.
	Cyber crisis management plan	0/1 (Not established)		Unpreparedness for managing large-scale cyber crises.
Legal Frameworks	Personal data protection legislation	0/1 (Not established)		Lack of a comprehensive legal basis for protecting personal data.

	Personal data protection authority	0/2 (Not established)		No independent body to oversee and enforce data protection.
Protection of Digital Services	Cyber security standard for public sector	0/2 (Not established)		Inconsistent security levels for digital services offered by Vatican entities.
Protection of Essential Services	Cyber security reqs. for essential services	0/2 (Not established)		Vital services may be vulnerable due to lack of mandated security measures.

This objective data from respected international bodies provides irrefutable evidence of the critical state of the Vatican's formal cybersecurity capabilities. The prevalence of zero scores across fundamental areas is a profound wake-up call, shifting the perception of the problem from subjective concern to objectively confirmed, critical deficiencies. The sophistication of documented attacks, such as the RedDelta campaign [22], when juxtaposed with these assessed defensive frailties, reveals a severe mismatch. This suggests that any current success in fending off advanced threats may be attributable more to fortune, the ad-hoc efforts of volunteers, or the specific security measures of individual departments rather than to systemic, institution-wide resilience.

C. Anatomy of a Prime Target: Why the Vatican is Uniquely Attractive to Threat Actors

The Vatican's unique status as a sovereign state, the headquarters of a global religion, a holder of immense historical and cultural treasures, and a significant diplomatic actor makes it an exceptionally attractive target for a diverse range of threat actors with varied motivations.

- **Geopolitical Espionage:** Nation-states are keenly interested in the Vatican's diplomatic positions, its intelligence on global affairs, internal Church governance, and its influence on Catholic populations worldwide. The RedDelta attack, aimed at gaining insight into negotiations with China [22], is a clear example of this threat.

The Holy See's Secretariat of State handles vast amounts of sensitive diplomatic communication [14], making it a prime target.

- **Financial Gain:** While the Vatican has made strides in financial reform through ASIF [16], its financial assets and the vast network of Catholic charitable giving can attract cybercriminals. Threats include ransomware attacks seeking extortion payments, business email compromise (BEC) scams targeting financial transfers (as seen in other religious organizations [27]), and theft of donor information for fraudulent purposes. Religious organizations, in general, are targeted for these reasons.[27]
- **Hacktivism and Ideological Attacks:** The Pope's global moral standing and the Church's positions on various social and political issues can provoke hacktivists or ideologically motivated groups. Their aims may include defacing prominent Vatican websites to spread a message, disrupting communications as a form of protest (potentially seen in the 2022 website outage [23]), or hijacking platforms to disseminate hostile content, as ISIS did with a church website.[27]
- **Data Theft for Influence or Compromise:** The personal data of high-ranking clergy, Vatican officials, and even ordinary faithful interacting with Vatican systems can be a target. Such data could be used for blackmail, to undermine the credibility of individuals or the institution, or to sow discord.
- **Disruption of Operations:** Attacks may simply aim to paralyze the Vatican's administrative functions, its global communication capabilities, or the operations of Vatican City State, causing chaos and reputational damage.
- **Compromise of Cultural Heritage:** The Vatican's digital and digitized archives, library collections, and museum data are invaluable. Threat actors could target these for theft (for sale on dark markets), ransom (as seen with the British Library [29]), or malicious alteration to damage or discredit historical records. State actors might target such institutions to attack a nation's or an institution's cultural identity.[30]

The Vatican's global moral and diplomatic influence also makes it a target for more insidious forms of attack, such as "perception hacking" or sophisticated disinformation campaigns. These aim to undermine its authority, manipulate public opinion, or sow discord among the faithful by compromising or spoofing its communication channels. The current infrastructure, with its documented weaknesses in threat analysis and incident response [26], may be ill-equipped to detect or counter such nuanced information operations that extend beyond traditional network intrusions.

The following table summarizes key Vatican digital assets and their associated cyber risks, illustrating the breadth and depth of what is at stake:

Table 2: The Vatican's Digital Assets & Associated Cyber Risks

Asset Category	Description & Significance	Primary Threat Vectors	Potential Impact of Compromise
Vatican Apostolic Archive & Library Digital Collections	Centuries of irreplaceable historical documents, papal records, manuscripts.[11] Global historical and cultural significance.	Ransomware, Data Theft, Malicious Alteration, Service Disruption	Loss/corruption of irreplaceable heritage, damage to scholarly research, reputational damage, loss of historical integrity.
Secretariat of State Diplomatic E-communications	Highly sensitive data related to international relations, negotiations, and Holy See foreign policy.[14]	Espionage (State-Sponsored), Data Theft, Man-in-the-Middle Attacks, Spear-Phishing	Diplomatic incidents, compromised negotiations, loss of trust with international partners, strategic disadvantage.
Holy See Financial Systems & Data	Financial records, transaction data, donor information, assets managed by entities like IOR and ASIF.[16]	Financial Fraud, Ransomware, Data Theft, BEC Attacks	Significant financial loss, disruption of financial operations, damage to donor confidence, regulatory scrutiny, reputational harm.
Vatican City State Operational Systems	Systems for managing museums, health services, infrastructure (e.g., Digital Twin of St. Peter's [7]), and other state functions.[6]	Service Disruption (DDoS), Ransomware, Data Breach, Sabotage	Paralysis of state functions, damage to critical infrastructure, public safety risks, loss of revenue (e.g., museum ticketing).
Dicastery Communication Platforms	Websites (e.g., vatican.va, vaticannews.va),	Defacement, DDoS, Disinformation Campaigns, Data	Disruption of global Church communication,

	email systems, internal communication networks used for global Church administration and evangelization.[2]	Interception, Account Compromise	spread of misinformation, erosion of trust, undermining of pastoral mission, reputational damage.
Personal Data of Clergy/Employees/Faithful	Sensitive personal identifiable information (PII), potentially including health, financial, and pastoral data.	Data Breach, Identity Theft, Phishing, Blackmail	Violation of privacy, identity theft, financial loss for individuals, erosion of trust in the Church, legal liabilities, reputational damage to the Vatican.

D. Echoes in Hallowed Halls: Lessons from Cyberattacks on Global Cultural and Religious Organizations

The cyber threats faced by the Vatican are not unique in type, though their potential impact is amplified by the Holy See's singular status. Examining attacks on other cultural and religious organizations provides sobering lessons and highlights common vulnerabilities.

The ransomware attack on the British Library in October 2023, perpetrated by the Rhysida gang, is a stark warning. This sophisticated attack resulted in the exfiltration of approximately 600GB of data, including personal data of users and staff, and the encryption or destruction of substantial portions of the Library's server estate.[29] Services were severely restricted for months, and the recovery was hampered by a reliance on legacy systems and a complex network topology that allowed attackers wider access. Key lessons from the British Library's transparent post-incident reporting include the critical need for comprehensive network monitoring, ubiquitous multi-factor authentication (MFA), regular in-depth security reviews, network segmentation, and well-practiced business continuity plans.[29]

Other cultural institutions have also fallen victim. The Grand Palais RMN in France suffered a ransomware attack during the 2024 Paris Olympics, affecting museum shops, including those at the Louvre. The Metropolitan Opera in New York experienced a data breach leaking personal data of over 45,000 people, disrupting ticketing operations.[30] Attacks on software providers like Gallery Systems and WordFly, which serve many cultural organizations, demonstrate the significant third-party risks inherent in the sector.[30] These incidents often exploit outdated infrastructure and under-resourced cybersecurity teams, characteristics that may resonate with parts of the Vatican's own complex and historically evolved IT environment.

Faith-based organizations (FBOs) globally are also increasingly in the crosshairs. They are vulnerable to ransomware, phishing, and data breaches, often due to limited IT resources and the exploitation of the inherent trust within these communities.[27] The Faith-Based Information Sharing and Analysis Organization (FB-ISAO) maintains an "ELEVATED" cyber threat level for FBOs, citing ongoing risks from hacktivism, BEC attacks, and ransomware, often exacerbated by geopolitical tensions and the public stances taken by FBOs or their personnel.[32] A recent report highlighted that the first quarter of 2025 saw a staggering doubling of ransomware attacks on non-profit organizations, including churches and religious centers, with prominent ransomware groups like Inc Ransom and RansomHub actively targeting this less-resourced sector.[33]

These global trends create a clear precedent: the Vatican is not an exception but a prime target within a broadly vulnerable ecosystem. However, its unique combination of spiritual authority, diplomatic weight, and unparalleled cultural heritage means the consequences of a successful major cyberattack would be exponentially more devastating than for a national library or a single religious charity. The Vatican cannot afford to benchmark its security against typical non-profits; it must aspire to a level of cyber resilience commensurate with its global stature and the potentially catastrophic, multi-dimensional impact of a major breach. The experiences of these other institutions serve as a direct and urgent warning.

III. The Indispensable Guardian: Why the Vatican Urgently Needs a Chief Information Security Officer (CISO)

The escalating digital threats and documented vulnerabilities confronting the Holy See demand a fundamental shift in its approach to cybersecurity. The current fragmented or ad-hoc measures are demonstrably insufficient. The establishment of a Chief Information Security Officer (CISO) role, and a supporting office, is not merely a technical upgrade but a strategic imperative for the Vatican to protect its mission, assets, and global standing in the 21st century.

A. Defining the CISO for the Vatican: Strategic Leader, Digital Guardian, Mission Enabler

For the Vatican, the CISO must be envisioned as far more than a technical manager. This role is that of a senior executive, responsible for developing and implementing an enterprise-wide information security vision, strategy, and program that safeguards all information assets and technologies from the full spectrum of threats.[34] The CISO is a leader who manages risks, aligns security posture with institutional objectives, and builds bridges between technical and non-technical stakeholders.[35]

In the unique context of the Holy See, the CISO would serve as a **Guardian of Digital Sovereignty**. This entails protecting the Vatican's unique information assets – from sacred archives to sensitive diplomatic communications – and ensuring its operational autonomy in the digital sphere, free from undue external influence or compromise.

Crucially, the CISO must also be a **Mission Enabler**. Effective cybersecurity is not an impediment to the Church's work but a vital support. By ensuring that digital transformation initiatives, global outreach, and administrative functions can proceed securely, the CISO enables the Vatican to leverage technology confidently for evangelization, communication, education, and the preservation of its heritage. This aligns with the perspective that cybersecurity can be an enabler of digital value, not merely a safeguard against threats, positioning the CISO as a steward of digital trust.[38]

Furthermore, a Vatican CISO must operate in profound alignment with the ethical framework articulated by the Holy See. Principles such as human dignity, the common good, ethical accountability, transparency, and robust data security, as emphasized in the Vatican's own AI Guidelines [8], must be woven into the fabric of the cybersecurity strategy. The AI Guidelines explicitly state that technology use should not harm the Pope's pastoral mission or compromise the Church [10]; the CISO would be a key figure in upholding this principle in the digital realm. This unique blend of responsibilities means a Vatican CISO cannot simply replicate a corporate model; the role must be deeply contextualized, requiring technical prowess, diplomatic acumen, cultural sensitivity, and a genuine understanding of the Church's universal mission.

B. Core Functions of a Vatican CISO Office: Tailored Responsibilities

Adapting standard CISO functions to the Vatican's specific context, a dedicated office would undertake the following core responsibilities:

1. **Strategic Governance & Policy Development:** Creating and enforcing a unified cybersecurity strategy, comprehensive policies, and clear standards applicable across the entire Holy See and Vatican City State. This includes all Dicasteries, administrative offices, and associated entities, ensuring a consistent and high level of security.[34] This would involve establishing clear leadership and accountability, assessing the current security posture, and fostering a security-first culture from the top down.[40]

2. **Comprehensive Cyber Risk Management:** Systematically identifying, evaluating, reporting on, and mitigating cyber risks to all categories of Vatican assets – spiritual, cultural, diplomatic, financial, and personal data.[34] This includes teaching personnel how to perform risk assessments and proposing safeguards, as outlined in ISO 27001 contexts.[41]
3. **Security Operations & Proactive Defense:** Overseeing robust threat detection, prevention mechanisms, continuous security monitoring, vulnerability management, and penetration testing. This would formalize, professionalize, and expand upon the valuable but limited work currently undertaken by volunteers like the Vatican CyberVolunteers.[1]
4. **Incident Response & Crisis Management:** Establishing and leading a centralized, coordinated response to cyberattacks and data breaches. This includes developing clear protocols, conducting regular drills, minimizing damage, ensuring swift recovery of systems and data, and managing internal and external communications during and after a crisis.[34]
5. **Data Governance, Privacy & Protection:** Championing the secure handling of all sensitive information, including diplomatic cables, financial records, the personal data of clergy and faithful, and the contents of the archives. This must be done in line with the ethical principles articulated in Vatican documents like the AI Guidelines [8] and evolving international data protection best practices.[34]
6. **Protection of Digital Cultural Heritage:** Developing and implementing specialized security strategies for the Vatican's irreplaceable digitized archives, libraries, and museum collections, in collaboration with the prefects and directors of these institutions. This includes ensuring the integrity and long-term preservation of digital assets.[7]
7. **Cybersecurity Awareness & Training:** Designing and delivering mandatory, ongoing cybersecurity training and awareness programs for all Vatican personnel, from Curial officials to administrative staff, to cultivate a deeply embedded security-conscious culture.[27]
8. **Vendor & Third-Party Risk Management:** Implementing rigorous processes for evaluating, selecting, and continuously monitoring the security practices of external service providers, software vendors, and other third-party contractors.[34] This is particularly critical given the observed reliance on contracted cybersecurity service providers without apparent third-party verification of their security setups.[1]
9. **Compliance & International Liaison:** Ensuring adherence to any applicable international regulations or standards and serving as the primary liaison with international cybersecurity bodies, national CERTs, and law enforcement agencies

on cybersecurity matters.

C. Addressing the Void: How a CISO Fills Critical Gaps

The functions of a CISO and their office directly address the profound cybersecurity deficiencies identified by international benchmarks and the experiences of the CyberVolunteers:

- The **lack of a coherent cybersecurity strategy and policy framework**, as highlighted by the NCSI [26], would be rectified by the CISO's primary responsibility to develop, implement, and oversee these foundational elements.
- The **critically low score for technical cybersecurity measures** noted by the ITU [1] would be tackled through the CISO's oversight of investment in, and proper configuration of, necessary security technologies and practices.
- The current **fragmented or unclear incident response capability**, implied by the NCSI's zero score for a national-level response unit [26], would be replaced by a CISO-led central command structure, ensuring coordinated and effective action during security incidents.
- The **absence of a dedicated cyber threat analysis unit** [26] would be filled by the CISO establishing robust threat intelligence capabilities tailored to the Vatican's unique threat landscape.
- The current **reactive security stance**, evidenced by the significant role of the CyberVolunteers in basic defense [1], would be transformed into a proactive, risk-based security posture driven by the CISO.
- The reported **lack of third-party checking on the security setups of contracted service providers** [1] would be addressed by the CISO implementing a formal vendor risk management program.

The absence of a CISO means that critical cybersecurity decisions are likely being made in silos by different directorates or dicasteries, or on an ad-hoc basis in response to immediate threats, or by individuals who may lack the strategic authority or holistic enterprise-wide view of risk. This inevitably leads to inconsistent levels of protection, inefficient allocation of resources, and a perpetual state of vulnerability. A CISO provides the unified vision, strategic direction, and empowered leadership necessary to overcome this fragmentation. Moreover, establishing a CISO is not merely about preventing attacks; it is fundamentally about building and maintaining digital trust. This includes the trust of the faithful that their interactions and data are handled securely, the trust of international partners in the confidentiality of diplomatic channels, and the trust of the global community in the integrity of the Vatican's vast repository of knowledge and heritage. A CISO, by professionalizing cybersecurity and demonstrably safeguarding these assets, plays a crucial role in upholding this multifaceted trust.

IV. Architecting Digital Sanctity: A Framework for the Vatican's CISO Office

Establishing a CISO office within the Vatican requires a bespoke governance model that respects its unique structure while ensuring effectiveness. It also necessitates the adaptation of global best practices and leveraging insights from comparable entities.

A. A Bespoke Governance Model: Integration, Independence, and Authority

A successful Vatican CISO office must be strategically positioned and adequately empowered.

- **Reporting Structure:** To ensure the necessary authority, visibility, and ability to drive institution-wide change, the CISO should report to a very senior level within the Vatican hierarchy. Options could include reporting directly to the Cardinal Secretary of State, or to a specially constituted committee within the Governorate of Vatican City State that includes key stakeholders from relevant dicasteries and directorates. This high-level reporting is consistent with best practices in complex organizations where CISOs often report to the CEO or the board to ensure cybersecurity is treated as a strategic priority.[35]
- **Integration with Existing Bodies:** The CISO office would not necessarily replace all existing IT and security functions but would provide strategic direction, oversight, and coordination. Clear lines of collaboration and defined responsibilities must be established with:
  - The Directorate of Telecommunications and Information Systems, particularly its CERT, which could evolve into a core component of a Vatican-wide Security Operations Center (SOC) under the CISO's strategic guidance.[6]
  - The Directorate of Security and Civil Protection Services, for coordinating on threats that bridge the physical and cyber domains, and leveraging their expertise in protective security.[18]
  - The Dicastery for Communication, regarding the security of the Holy See's extensive communication networks and online presence.[4]
  - The new AI Commission, ensuring that cybersecurity considerations are integral to AI governance and deployment.[8]
  - The Supervisory and Financial Information Authority (ASIF), for aligning on the protection of financial systems and data.[16]
- **Lessons from ASIF's Success:** The establishment and evolution of ASIF offer a powerful internal precedent for creating an effective, independent oversight body within the Vatican.[16] ASIF's journey from addressing financial scandals to

becoming a respected regulator demonstrates the Holy See's institutional capacity for significant structural reform when faced with critical risks and the need to meet international standards. Key elements of ASIF's success that a CISO office could emulate include its operational independence, a clear and robust mandate, strong leadership, a tripartite structure (e.g., for policy/governance, operations/incident response, and risk/compliance), active international collaboration, the incorporation of external expertise, and a commitment to continuous improvement and proactive governance.[16] This precedent counters potential arguments that the Vatican is inherently resistant to or incapable of such modernization in critical governance areas.

- **Necessary Independence and Resources:** The CISO office must be granted sufficient autonomy to make objective security assessments and enforce policies across diverse Vatican entities. Crucially, it requires an adequate and sustained budget to acquire necessary technologies and, most importantly, to attract and retain skilled cybersecurity personnel – a significant challenge in a competitive global market. The CISO must have the authority to mandate security controls and protocols institution-wide.[34]

This governance model must also be designed with an understanding of "subsidiarity," a key principle in Catholic social teaching. While the CISO office would provide centralized strategy, overarching policies, shared services (like advanced threat intelligence or a central SOC), and critical incident command, individual Dicasteries and entities could retain responsibility for managing the specific operational security needs of their unique systems, albeit within the unified framework and subject to audit and oversight by the CISO. This approach fosters buy-in, leverages local expertise, and respects the diverse operational contexts within the Vatican, balancing central control with distributed responsibility.

B. Pillars of a Resilient Digital Vatican: Adapting Global Best Practices

The Vatican CISO office should build its strategy upon globally recognized cybersecurity frameworks, tailored to the Holy See's unique context.

- **Comprehensive Risk Management Framework:** Adopting a structured approach to risk management, such as that outlined in the NIST Cybersecurity Framework (CSF) [40] or ISO 27001.[36] This framework must be customized to address the Vatican's specific threat landscape, which includes geopolitical espionage, sophisticated financial crime, hacktivism, and threats to its spiritual and cultural mission. NIST CSF 2.0, with its expanded "Govern" function, is particularly relevant for establishing strong CISO leadership and integrating cybersecurity into the Vatican's overall governance.[38]

- **Proactive Threat Intelligence and Counter-Espionage Capabilities:** Developing an internal or partnered capability to gather, analyze, and act upon threat intelligence specific to actors and campaigns targeting the Holy See. Given the documented state-sponsored threats [22], this function is critical.
- **Robust Incident Response and Crisis Management:** Establishing clear, documented, and regularly practiced incident response plans. This includes defining roles and responsibilities, communication protocols, technical containment strategies, and processes for business continuity and disaster recovery to ensure the resilience of critical Vatican operations.[36]
- **Data Governance, Privacy, and Protection Program:** Implementing comprehensive policies and technical controls for the classification, handling, storage, and transmission of all sensitive data. This program must be consistent with the ethical principles articulated in Vatican documents, such as the AI Guidelines' emphasis on human dignity and data security [8], and should draw from international data protection standards like GDPR where appropriate.
- **Cultivating a Cyber-Aware Culture:** Implementing mandatory and continuous cybersecurity awareness training for all officials, clergy, and staff across all Curial bodies and Vatican City State entities. This training should cover topics like phishing recognition, strong password practices, secure handling of information, and reporting suspicious activities.[27]
- **Specialized Protection for Digital Cultural Heritage:** Working closely with the custodians of the Vatican Apostolic Archive, Apostolic Library, Museums, and other cultural entities to develop and implement specific cybersecurity protocols for their invaluable digital and digitized collections. This includes secure digitization processes, robust metadata management, protection against data degradation or malicious alteration, and secure long-term digital preservation strategies.[7] The Vatican Apostolic Library's existing work on long-term digital preservation (LTDP), focusing on quality control, format sustainability, and technical protection mechanisms [44], provides a foundation to build upon.
- **Ensuring Compliance and Fostering International Cybersecurity Cooperation:** Monitoring and ensuring adherence to any relevant international cybersecurity standards or legal obligations. The CISO office should also actively engage with global cybersecurity initiatives, national CERTs, and law enforcement agencies to share information (where appropriate) and collaborate on combating transnational cyber threats, expanding on the Vatican's current minimal representation in such forums.[26]

The following table outlines a proposed mandate for a Vatican CISO office, linking functions to best-practice frameworks and key internal stakeholders:

Table 3: Proposed Mandate and Key Responsibilities for the Vatican CISO Office

Core CISO Office Function	Specific Responsibilities Tailored to the Vatican	Alignment with Best-Practice Frameworks (Examples)	Key Vatican Stakeholders/Collaborators
Strategic Governance & Policy	Develop, implement, and enforce Holy See-wide cybersecurity directives, standards, and architecture, respectful of unique Dicastery needs and aligned with Vatican ethical principles.[8]	NIST CSF: Govern, Identify; ISO 27001: Clauses 5, 6	Secretary of State, Governorate, Pontifical Commission for Vatican City State, Heads of Dicasteries.
Cyber Risk Management	Establish and manage an enterprise-wide cyber risk assessment program; identify and prioritize threats to spiritual, cultural, diplomatic, and financial assets; report risks to senior leadership.[34]	NIST CSF: Identify, Protect; ISO 27001: Clause 8	All Dicasteries and Vatican City State entities, ASIF, Directorate of Security.
Security Operations & Incident Response	Oversee threat detection, vulnerability management, security monitoring; lead centralized response to cyber incidents, coordinating containment, eradication, and	NIST CSF: Protect, Detect, Respond, Recover	Directorate of Telecommunications (CERT), Directorate of Security, Dicastery for Communication, all affected entities.

	recovery efforts.[1]		
Data Protection & Privacy	Develop and enforce policies for secure handling of personal data (clergy, faithful, employees), diplomatic records, and financial information, aligning with Vatican ethics and relevant standards.[8]	NIST Privacy Framework; ISO 27001: Annex A.18	Secretariat of State, Dicastery for the Doctrine of the Faith, Dicastery for Evangelization, ASIF, Health Services.
Digital Cultural Heritage Security	Oversee security of Vatican Apostolic Archive/Library digitization, digital preservation, and access systems; collaborate with Prefects/Librarians on specialized protection strategies.[11]	NIST CSF: Protect, Identify; ISO 27001 (relevant controls)	Vatican Apostolic Archive, Vatican Apostolic Library, Vatican Museums, Fabbrica di San Pietro.
Cybersecurity Training & Awareness	Design and implement mandatory, ongoing cybersecurity awareness programs for all Vatican personnel to foster a security-conscious culture.[27]	NIST CSF: Protect (Awareness & Training)	All Vatican personnel, Human Resources departments.
Third-Party Risk Management	Establish processes for cybersecurity risk assessment of all third-party vendors, contractors, and cloud service providers; ensure contractual security	NIST CSF: Identify (Supply Chain Risk Management)	All entities engaging third parties, Procurement offices.

	requirements.[1]		
International Liaison & Compliance	Represent the Holy See in global cybersecurity forums; manage relations with national CERTs and law enforcement on cyber matters; monitor and ensure compliance with relevant international standards.[26]	(International cooperation aspects)	Secretariat of State (Section for Relations with States), Directorate of Telecommunications.

C. Leveraging International Frameworks and Models

The Vatican is not alone in facing the challenge of establishing robust cybersecurity governance. It can draw upon established international frameworks and observe the approaches of other, particularly smaller or unique, states.

- **NIST Cybersecurity Framework (CSF):** This voluntary framework, developed by the U.S. National Institute of Standards and Technology, provides a high-level structure of standards, guidelines, and best practices to manage cybersecurity risk.[40] Its core functions—Identify, Protect, Detect, Respond, Recover—and the new "Govern" function in CSF 2.0, offer a comprehensive roadmap.[39] The "Govern" function is particularly pertinent as it emphasizes establishing and monitoring the organization's cybersecurity risk management strategy, expectations, and policy, directly supporting the CISO's mandate.[39]
- **ISO/IEC 27001:** This international standard specifies the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS).[36] Adopting or aligning with ISO 27001 would provide the Vatican with a systematic approach to managing sensitive company information so that it remains secure. It includes requirements for risk assessment and treatment, security controls, and continuous improvement.[41]
- **Cybersecurity Governance in European Microstates:** While direct comparisons are imperfect, the experiences of European microstates in establishing national cybersecurity capabilities can offer insights.
  - **Monaco:** The Principality established the Agence Monégasque de Sécurité Numérique (AMSN) in December 2015.[45] AMSN is the national authority for information system security, with missions including preventing, detecting, and handling cyberattacks; crisis reaction; IT product certification; representing Monaco in international digital security bodies; and raising

    awareness among public services and Operators of Vital Importance (OIVs).[45] Monaco is also voluntarily aligning its cybersecurity framework with the EU's NIS2 Directive, demonstrating a proactive approach to adopting robust regional standards despite not being legally bound.[46] This provides a model of a small state creating a dedicated agency with a broad mandate.
  - **Liechtenstein:** Established a National Cybersecurity Unit between 2020 and 2021, serving as a central office for all matters related to cyber risks and as an intermediary for the public, companies, critical infrastructure operators, and authorities.[47] These examples show that even small sovereign entities recognize the need for centralized cybersecurity leadership and coordination.
- **UNESCO Guidelines for Cultural Heritage and Digital Safety:** UNESCO has been active in promoting the protection and promotion of diverse cultural expressions in the digital environment and developing guidelines for regulating digital platforms to ensure an open, safe, and secure online environment, while upholding human rights.[48] These principles and frameworks are highly relevant to the Vatican's mission to protect its vast cultural and documentary heritage in digital forms and to ensure its global communications are secure and trustworthy.

By drawing on these frameworks and models, the Vatican can develop a CISO office and cybersecurity strategy that is both grounded in global best practices and uniquely tailored to its own sacred mission and complex operational environment. Such an approach also enhances the Vatican's credibility as a global actor. Effective cybersecurity is not merely a defensive posture; it is a critical component of its "digital diplomacy" and its ability to engage confidently and securely on the world stage.

V. Navigating the Path Forward: Embracing Digital Resilience for a Timeless Mission

The establishment of a CISO office within the Vatican, while crucial, will undoubtedly present challenges. However, by framing this initiative as a strategic enabler and a moral imperative, these hurdles can be overcome, paving the way for enhanced digital resilience that supports the Holy See's timeless mission.

A. Anticipating and Addressing Challenges: Culture, Structure, and Resources

Several potential challenges must be anticipated and proactively addressed:

- **Cultural Resistance:** Ancient institutions, by their nature, can be deliberate in adopting change. The Vatican's cautious, human-centric approach to technology is evident in its AI Guidelines, which emphasize that "technological innovation cannot and should never overtake or replace human beings".[9] This deeply held value must be respected. The introduction of a CISO and new cybersecurity protocols might be perceived by some as an impediment to work, a purely technical cost center, or an unwelcome layer of bureaucracy. Overcoming this requires careful communication, emphasizing cybersecurity as an enabler of the mission, not a hindrance. Past Vatican communication reforms highlighted a risk of focusing on technical details over mission and content, a pitfall the CISO implementation must avoid by clearly linking security to the Vatican's core objectives.[50]

- **Structural Inertia:** Integrating a new, authoritative office like that of a CISO into the long-established and complex structures of the Roman Curia and Vatican City State will require careful planning and strong leadership. Past reforms, such as those in finance and the Curia itself, have encountered internal resistance and highlighted the complexities of effecting change within the Vatican's unique environment.[51] Clearly defined roles, responsibilities, and lines of authority for the CISO will be essential to avoid "turf wars" and ensure effective collaboration with existing directorates and dicasteries.
- **Resource Allocation:** A fully functional CISO office and the implementation of a comprehensive cybersecurity strategy will require significant and sustained financial investment in technology, processes, and, most importantly, skilled personnel. In an environment with numerous competing priorities, securing this funding may be challenging. However, the potential cost of a major cyber incident – including financial loss, operational disruption, reputational damage, and the compromise of irreplaceable heritage – far outweighs the proactive investment in security.[53]
- **Talent Acquisition and Retention:** Attracting and retaining cybersecurity professionals with the requisite high-level technical skills, discretion, and cultural sensitivity to operate effectively within the Vatican environment will be a key challenge. The global demand for cybersecurity talent is high, and the Vatican will need to offer a compelling value proposition.

The Vatican's recent and sophisticated engagement with AI ethics and governance, as demonstrated by its detailed AI guidelines [8], reveals an existing institutional capacity for profound thinking about technology's impact. This intellectual framework can be powerfully leveraged to build support for a CISO. Robust cybersecurity is, after all, a prerequisite for ethical AI and the development of trustworthy digital systems. If the Vatican is committed to the principles of ethical technology use, it must also commit to the foundational cybersecurity that makes such use possible and safe.

B. The CISO as a Strategic Enabler: Beyond a Cost Center

It is crucial to frame the CISO role not as a mere cost center or a department of "no," but as a strategic enabler that actively supports and enhances the Vatican's mission and operations:

- **Protecting Mission Continuity:** A core function of the CISO is to ensure that the Vatican's global operations – pastoral, administrative, diplomatic, and charitable – can continue without disruption from cyber threats. This resilience is fundamental to the Church's ability to function effectively in the modern world.
- **Enabling Digital Transformation Safely:** The Vatican is already embracing digital transformation, from the use of AI [8] to the digitization of its vast library and archives using technologies like Web3.[13] A CISO provides the security foundation that allows the Holy See to confidently adopt and expand these new technologies for evangelization, global communication, education, and heritage preservation, without undue risk.
- **Enhancing Trust and Credibility:** In an age of widespread concern about data privacy and digital security, a demonstrable commitment to robust cybersecurity, led by a professional CISO, significantly enhances the Vatican's trustworthiness. This applies to the personal data of the faithful, the confidentiality of diplomatic exchanges, and the integrity of its historical and cultural assets. As highlighted by the DVMS Institute's work on NIST CSF 2.0, cybersecurity is an "enabler of digital business value" and CISOs are "stewards of digital trust".[38]
- **Supporting Financial Integrity and Transparency:** Strong cybersecurity is intrinsically linked to protecting financial systems, data, and transactions. The CISO's work would directly complement and reinforce the efforts of ASIF to ensure financial integrity and combat illicit financial activities within the Vatican.[16]

Overcoming cultural and structural inertia will require framing cybersecurity not as an isolated technical concern, but as a fundamental component of institutional integrity, comprehensive risk management, and successful mission fulfillment. This necessitates visible leadership and sustained commitment from the highest levels of the Vatican.

C. The Moral and Operational Imperative: A Call to Stewardship

Ultimately, the establishment of a CISO office is a moral and operational imperative, deeply aligned with the Vatican's core values and responsibilities:

- **Stewardship of Heritage:** The Holy See is the custodian of an unparalleled patrimony of historical, cultural, and spiritual treasures. As these are increasingly digitized, the responsibility of stewardship extends with equal force to their digital forms. Protecting these digital assets from loss, corruption, or malicious alteration is a profound duty.

- **Protecting the Faithful:** The Vatican has a moral obligation to safeguard the personal data and digital interactions of Catholics worldwide who engage with the Holy See's online services, participate in Church initiatives, or whose information is held within its systems. This aligns directly with the principles of protecting human dignity and the common good, as articulated in the AI Guidelines.[8]
- **Ensuring the Church's Unfettered Voice:** The integrity and availability of the Vatican's communication channels are vital for proclaiming its message, providing pastoral guidance, and engaging in dialogue globally. Cybersecurity ensures that this voice cannot be easily silenced, manipulated, or discredited by malicious actors.
- **Prudence and Preparedness:** In the face of clearly documented and escalating cyber threats, the ethical obligation of prudence demands that the Vatican take all reasonable and robust measures to defend itself and its assets. Preparedness is not just a technical requirement but an expression of responsible governance.

The global nature of the Catholic Church means that a significant cyber incident at the Vatican could have far-reaching and damaging consequences for dioceses, religious orders, and Catholic institutions worldwide. Many of these entities may look to the Holy See for guidance and are themselves vulnerable, often with even fewer resources. A well-established Vatican CISO office, after maturing its own capabilities, could eventually play a vital role in fostering broader cybersecurity resilience across the global Church. This could involve sharing threat intelligence, developing best practice guidelines, or offering expert advice, thereby allowing the Holy See to lead by example and extend a protective umbrella of cybersecurity knowledge and support to the wider Catholic community.

Conclusion: A Fervent Call to Action – Securing the Vatican for Today and for Posterity

The Holy See, a beacon of faith and a venerable institution of immense historical, cultural, and diplomatic significance, stands at a critical juncture in the digital age. Its expanding reliance on digital infrastructure, while essential for its global mission and the preservation of its unique heritage, has concurrently exposed it to a sophisticated and escalating array of cyber threats. The evidence is undeniable: from targeted state-sponsored espionage like the RedDelta campaign [22] to disruptive website outages [23] and the alarming 150% rise in attacks reported by the Vatican CyberVolunteers.[1] International benchmarks, such as the ITU Global Cybersecurity Index and the National Cyber Security Index, deliver a sobering verdict, placing

Vatican City State among the lowest performers globally in technical cybersecurity measures and foundational governance capabilities.[1]

The current approach to cybersecurity within the Vatican, characterized by dedicated but often siloed efforts and a significant reliance on volunteer initiatives, is insufficient to counter the magnitude and complexity of these threats. It is a posture that is unsustainable in the face of adversaries who are persistent, well-resourced, and strategically motivated to target the Holy See's invaluable assets – assets that range from the irreplaceable contents of the Vatican Apostolic Archive [11] and Library [13] to sensitive diplomatic communications [14], financial data [16], and the personal information of millions of faithful.

The decision to establish a robust, professionally staffed, and strategically empowered Chief Information Security Officer (CISO) office is therefore not merely a technical or administrative adjustment; it is a profound act of modern stewardship. It is the 21st-century equivalent of the centuries of meticulous effort dedicated to preserving the Vatican's physical treasures and safeguarding its doctrinal integrity. It is an acknowledgment that in an interconnected world, digital security is inextricably linked to institutional sovereignty, operational resilience, and the unwavering trust placed in the Holy See by over a billion people worldwide.

Failure to act decisively risks a future where the Vatican could lose control over its own narrative, see its historical record compromised, or find its ability to communicate freely and securely impeded. This would represent a ceding of a degree of its sovereignty not to a traditional temporal power, but to unseen and often malicious digital forces. The potential consequences – diplomatic, financial, reputational, and indeed, spiritual – are too grave to contemplate.

Therefore, this analysis concludes with a fervent but respectful call to the leadership of the Holy See and Vatican City State. The time for incremental adjustments or reliance on provisional measures has passed. The moment demands decisive action: the immediate commitment to establish a CISO office with the authority, resources, and mandate to architect and implement a comprehensive, enterprise-wide cybersecurity strategy. This is not just about protecting data; it is about safeguarding a legacy, ensuring the continuity of a global mission, and fortifying the Vatican for the challenges and opportunities of today, and for posterity. As one who has witnessed the digital siege firsthand, the urgency of this call cannot be overstated. The digital gates of the Vatican must be secured with the same diligence and dedication afforded to its most sacred physical precincts.

Sources

1. The Vatican's cyber crusaders - Politico.eu, geopend op mei 27, 2025, https://www.politico.eu/article/vatican-cyber-group-vigilantes-digital-attacks-pope/
2. Vatican Internet Sites - The Holy See, geopend op mei 27, 2025, https://www.vatican.va/siti_va/index_va_en.htm
3. The Holy See, geopend op mei 27, 2025, https://www.vatican.va/
4. Profile - Dicastero per la Comunicazione, geopend op mei 27, 2025, https://www.comunicazione.va/en/chi-siamo/profilo.html
5. Dicastery for Communication - The Holy See, geopend op mei 27, 2025, https://www.vatican.va/content/romancuria/en/dicasteri/dicastero-per-la-comunicazione/profilo.html
6. Directorate of Telecommunications and Information Systems, geopend op mei 27, 2025, https://www.vaticanstate.va/en/directorates/directorate-of-telecommunications-and-information-systems.html
7. New Pope, Ancient Basilica: How a Digital Twin Helps Protect the Vatican's Majestic Church | Bentley Blog | Infrastructure Engineering Software & Solutions, geopend op mei 27, 2025, https://blog.bentley.com/insights/new-pope-ancient-basilica-how-a-digital-twin-helps-protect-the-vaticans-majestic-church/
8. The guidelines on AI 2025 | Vatican - Digital Watch Observatory, geopend op mei 27, 2025, https://dig.watch/resource/the-guidelines-on-ai-2025-vatican
9. Vatican City State puts AI guidelines in place | USCCB, geopend op mei 27, 2025, https://www.usccb.org/news/2025/vatican-city-state-puts-ai-guidelines-place
10. The Principles behind the Guidelines on Artificial Intelligence, geopend op mei 27, 2025, https://www.vaticanstate.va/en/news/1372-the-principles-behind-the-guidelines-on-artificial-intelligence.html
11. Vatican Apostolic Archive - Wikipedia, geopend op mei 27, 2025, https://en.wikipedia.org/wiki/Vatican_Apostolic_Archive
12. The Most Secure Buildings | 3: The Vatican Archives - American Guard Services, Inc., geopend op mei 27, 2025, https://americanguardservices.com/news/the-most-secure-buildings-3-the-vatican-archives/
13. Where Ancient Heritage Meets Modern Technology: Why The Vatican Library Is Embracing Web3 - Forbes Africa, geopend op mei 27, 2025, https://www.forbesafrica.com/life/2025/01/06/where-ancient-heritage-meets-modern-technology-why-the-vatican-library-is-embracing-web3/
14. Secretariat of State (Holy See) - Wikipedia, geopend op mei 27, 2025, https://en.wikipedia.org/wiki/Secretariat_of_State_(Holy_See)
15. The Vatican Files - Franklin D. Roosevelt Library & Museum, geopend op mei 27, 2025, http://docs.fdrlibrary.marist.edu/vatican.html
16. Pope Leo XIV: Financial crime champion? What global compliance ..., geopend op

mei 27, 2025, https://vinciworks.com/blog/pope-leo-xiv-financial-crime-champion-what-global-compliance-teams-can-learn-from-the-vaticans-fight-against-corruption/

17. Direction des Télécommunications et des Systèmes informatiques, geopend op mei 27, 2025, https://www.vaticanstate.va/fr/directions/direction-des-telecommunications-et-des-systemes-informatiques.html
18. Gianluca Gauzzi Broccoletti - Wikipedia, geopend op mei 27, 2025, https://en.wikipedia.org/wiki/Gianluca_Gauzzi_Broccoletti
19. Conclave: A Look at Security Around the Secretive Election Process - ASIS International, geopend op mei 27, 2025, https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2025/may/Conclave-Security/
20. Vatican security for conclave 'sets a gold standard' for organizations, says expert, geopend op mei 27, 2025, https://www.detroitcatholic.com/news/vatican-security-for-conclave-sets-a-gold-standard-for-organizations-says-expert
21. Vatican allegedly hacked by China ahead of key talks | PBS News, geopend op mei 27, 2025, https://www.pbs.org/newshour/world/vatican-allegedly-hacked-by-china-ahead-of-key-talks
22. Chinese State-Sponsored Group 'RedDelta' Targets the Vatican and ..., geopend op mei 27, 2025, https://www.recordedfuture.com/research/reddelta-targets-catholic-organizations
23. Even the Vatican Is Vulnerable to Cyberattack | Core Managed IT Services, geopend op mei 27, 2025, https://coremanaged.com/even-the-vatican-is-vulnerable-to-cyberattack/
24. Vatican news services hit by internet outages | News Headlines - Catholic Culture, geopend op mei 27, 2025, https://www.catholicculture.org/news/headlines/index.cfm?storyid=64051
25. Who are the Vatican's "digital guardians" protecting it from cyberattacks? "We are the digital version of the Swiss Guard" - Free Press, geopend op mei 27, 2025, https://www.slobodenpecat.mk/en/koi-se-digitalnite-chuvari-na-vatikan-shto-go-shtitat-od-kibernapadi-nie-sme-digitalna-verzija-na-shvajcarskata-garda/
26. Vatican City - NCSI, geopend op mei 27, 2025, https://ncsi.ega.ee/country/va_2022/?allData=1
27. HOW TO PROTECT YOUR CHURCH OR MINISTRY AGAINST CYBERATTACKS - GuideStone, geopend op mei 27, 2025, https://www.guidestone.org/-/media/Landing-Pages/Property-and-Casualty/Cybersecurity-White-Paper.ashx
28. Safeguarding the Faith-Based Sector from Growing Cyber Threat - DataGuard, geopend op mei 27, 2025, https://data-guard365.com/articles/safeguarding-the-faith-based-sector-from-growing-cyber-threats/

29. British Library Cyber Attack - 10 Lessons - Cyber Security - I by IMD, geopend op mei 27, 2025, https://www.imd.org/ibyimd/technology/full-transparency-10-lessons-from-the-cyber-attack-on-the-british-library/
30. Security Gaps in Cultural Institutions - threatER, geopend op mei 27, 2025, https://www.threater.com/blog/security-gaps-in-cultural-institutions/
31. Cybersecurity Checklist for Church, School, & Nonprofit - Beacon Insurance Agency, geopend op mei 27, 2025, https://trustbia.com/cybersecurity-checklist-for-church-school-nonprofit/
32. FB-ISAO Current Threat Level, geopend op mei 27, 2025, https://faithbased-isao.org/fb-isao-current-threat-level/
33. 2025 Q1 Ransomware & Cyber Threat Report | GuidePoint Security, geopend op mei 27, 2025, https://www.guidepointsecurity.com/wp-content/uploads/2025/04/GRIT-2025-Q1-Ransomware-Cyber-Threat-Report.pdf
34. The Role of a Chief Information Security Officer in Today's Information Landscape, geopend op mei 27, 2025, https://www.digitalguardian.com/blog/role-chief-information-security-officer-todays-information-landscape
35. The CISO Role: What Does a Chief Information Security Officer Do? - Splunk, geopend op mei 27, 2025, https://www.splunk.com/en_us/blog/learn/chief-information-security-officer-ciso-role.html
36. Chief information security officer - Wikipedia, geopend op mei 27, 2025, https://en.wikipedia.org/wiki/Chief_information_security_officer
37. Chief Information Security Officer (CISO) - BlackFog, geopend op mei 27, 2025, https://www.blackfog.com/cybersecurity-101/chief-information-security-officer-ciso/
38. dvmsinstitute.com, geopend op mei 27, 2025, https://dvmsinstitute.com/2025/05/01/how-cisos-can-earn-a-seat-in-the-boardroom-using-a-nist-cybersecurity-framework-digital-value-management-system/#:~:text=Value%20Creation%20and%20Protection%3A%20The%20CISO's%20New%20Mandate&text=It%20views%20cybersecurity%20as%20an,the%20value%20creation%20lifecycle%E2%80%8B.
39. How CISOs can Earn a Seat in the Boardroom Using a NIST Cybersecurity Framework Digital Value Management System - DVMS institute, geopend op mei 27, 2025, https://dvmsinstitute.com/2025/05/01/how-cisos-can-earn-a-seat-in-the-boardroom-using-a-nist-cybersecurity-framework-digital-value-management-system/
40. Effective Cybersecurity Governance: Best Practices for 2025 - Prey, geopend op mei 27, 2025, https://preyproject.com/blog/cybersecurity-governance-best-practices
41. What is the job of Chief Information Security Officer (CISO) in ISO 27001? - Advisera, geopend op mei 27, 2025, https://advisera.com/27001academy/knowledgebase/what-is-the-job-of-chief-in

formation-security-officer-ciso-in-iso-27001/

42. 2023 Volume 5 Improving Information Security Through Organizational Change - ISACA, geopend op mei 27, 2025, https://www.isaca.org/resources/isaca-journal/issues/2023/volume-5/improving-information-security-through-organizational-change
43. Leveraging NIST CSF for Public Sector Cybersecurity - Semperis, geopend op mei 27, 2025, https://www.semperis.com/blog/leveraging-nist-csf-for-public-sector-cybersecurity/
44. HARING, PRESERVING AND EXPLOITING DIGITAL COLLECTIONS AT THE VATICAN LIBRARY - Conservation Science in Cultural Heritage, geopend op mei 27, 2025, https://conservation-science.unibo.it/article/download/20046/18216/81592
45. Agence Monégasque de Sécurité Numérique / Ministère d'État / Le ..., geopend op mei 27, 2025, https://www.gouv.mc/Gouvernement-et-Institutions/Le-Gouvernement/Ministere-d-Etat/Agence-Monegasque-de-Securite-Numerique
46. NIS2 directive regulations and implementation in Monaco - CyberUpgrade, geopend op mei 27, 2025, https://cyberupgrade.net/blog/compliance-regulations/nis2-directive-regulations-and-implementation-in-monaco/
47. Governance - Liechtenstein | Interoperable Europe Portal - European Union, geopend op mei 27, 2025, https://interoperable-europe.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/governance-liechtenstein
48. The Government of Canada calls for stronger international cooperation on digital governance at UNESCO - Canada.ca, geopend op mei 27, 2025, https://www.canada.ca/en/canadian-heritage/news/2025/02/the-government-of-canada-calls-for-stronger-international-cooperation-on-digital-governance-at-unesco.html
49. Guidelines for the Governance of Digital Platforms - UNESCO, geopend op mei 27, 2025, https://www.unesco.org/en/internet-trust/guidelines
50. Pope Francis: The Steps of Vatican Reform - MondayVatican, geopend op mei 27, 2025, https://www.mondayvatican.com/vatican/pope-francis-the-steps-of-vatican-reform
51. Francis's Legal Revolution: A Reforming Impulse with Many Lights and Some Shadows, geopend op mei 27, 2025, https://talkabout.iclrs.org/2025/04/22/franciss-legal-revolution/
52. What happens now with Pope Francis's “unfinished business”? - Exaudi, geopend op mei 27, 2025, https://www.exaudi.org/what-happens-now-with-pope-franciss-unfinished-business/
53. Cybercrime To Cost The World $10.5 Trillion Annually By 2025, geopend op mei 27, 2025, https://cybersecurityventures.com/cyberwarfare-report-intrusion/
54. Cybercrime To Cost The World $10.5 Trillion Annually By 2025, geopend op mei

27, 2025,
https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/