Introduction

This paper explores the critical importance of data protection and privacy for churches and nonprofits. It emphasizes the necessity of safeguarding personal information to maintain stakeholder trust and institutional integrity. By securely managing sensitive data, these ministries can prevent unauthorized access and breaches. Effective data protection is essential not only for regulatory compliance but also for preserving community trust.

This paper will first highlight the importance of data protection and privacy, then define these concepts, and finally delve into four key risk areas: reputational risks, financial risks, operational risks, and institutional risks. By addressing these risks, ministries can cultivate a culture of privacy that aligns their missions with principles of transparency and integrity.

Importance of Data Protection and Privacy

Data protection and privacy are essential for securing sensitive information from unauthorized access and breaches. Unfortunately, churches and ministries often overlook these critical measures, whether intentionally or unintentionally. By implementing robust data management practices, they can ensure compliance with regulations and maintain the trust of their stakeholders. Prioritizing data protection not only upholds ethical standards but also strengthens relationships within the community. This motivation drives me to write this paper, highlighting the importance of these often-neglected practices.

Firstly, this paper will start by defining what data protection and privacy mean. Next, it will explore their relevance to churches and nonprofits. Then, the paper will discuss the impact of data protection on trust and integrity with stakeholders. Finally, it will emphasize the importance of prioritizing these measures to uphold ethical standards and strengthen community relationships.

Definition of Data Protection and Privacy

Data protection refers to the legal rules that control how personal information is processed, ensuring it is handled fairly, legally, and transparently. Privacy, on the other hand, is the right to be left alone and to manage one's own personal information. As Peter Blume notes, “Data protection is specifically related to the legal rules that regulate to which extent and under which conditions information related to individual physical persons may be used” (Blume, 1999, p. 153). Privacy is described as "a personal condition of life characterised by seclusion from, and therefore absence of acquaintance by, the public" (de Andrade, 2017, p. 5).

Relevance to Churches and Nonprofits

Many of us often confuse data with personal information and struggle with how to collect, store, and use it, especially in churches and nonprofits. Data protection refers to the legal rules that control how personal information is processed, ensuring it is handled fairly, legally, and transparently. Privacy, on the other hand, is the right to be left alone and to manage one's own personal information. As Peter Blume notes, “Data protection is specifically related to the legal rules that regulate to which extent and under which conditions information related to individual physical persons may be used” (Blume, 1999, p. 153). Privacy is described as "a personal condition of life characterised by seclusion from, and therefore absence of acquaintance by, the public" (de Andrade, 2017, p. 5).

Impact on Trust and Integrity with Stakeholders

Effective data protection and privacy practices are crucial for churches and nonprofits, as they significantly enhance trust and integrity between ministries and their stakeholders. These practices must be timely, updated, and accurate. When stakeholders feel confident that their personal information is secure and their privacy respected, their trust in the ministry grows. Norberto Andrade emphasizes that "data protection is only a tool at the service of our dignity and liberties and not a value as such" (Poullet, 2010, as cited in de Andrade, 2017). This statement highlights the importance of data protection in maintaining institutional integrity and ethical standards, thereby fostering trustworthy relationships with stakeholders.

Reputational Risk Management

Addressing data protection and privacy risks is vital for maintaining stakeholder trust. This section explores various types of data risks, including personal data breaches, unauthorized access, and data loss. We identify sources of these risks, such as employee negligence and cyberattacks. Effectively communicating data protection efforts fosters transparency and builds trust with stakeholders. Key areas covered include Types of Data Risk, Data Loss and Corruption, and Communicating Data Protection Efforts.

Understanding Data Protection and Privacy Risks

Effectively managing data protection and privacy risks is crucial for maintaining stakeholder trust and organizational integrity. This section will explore various types of data risks, including personal data breaches, unauthorized access and cyber threats, and data loss and

corruption, as well as common sources of these risks, such as internal threats like employee negligence, external threats like cyberattacks, and vulnerabilities from third-party vendors and partnerships.

Types of Data Risk

Entities face significant data risks that threaten the integrity and confidentiality of personal information in today's digital landscape. These risks fall into internal and external categories. Internal threats often stem from "employee negligence," leading to unauthorized access or data breaches (Solove, 2024). External threats primarily consist of "cyberattacks" that exploit system vulnerabilities (Solove, 2024). Additionally, "third-party vendors and partnerships" complicate data security, as they may lack stringent safeguards (Solove, 2024). Understanding these sources—such as data loss, corruption, and unauthorized access—is crucial for developing effective mitigation strategies.

Personal Data Risks

Personal data risks are complex in today's digital landscape. Defined as "any data that relates to an identifiable person," personal data is susceptible to threats like unauthorized access and data breaches (Cha & Yeh, 2018). Proper classification of these risks is essential, as incidents involving personal data can escalate and have recently contributed to the loss of millions of records (Cha & Yeh, 2018, p. 50510). It is crucial to implement effective security measures. According to Dokuchaev et al. (2020), understanding threats is vital for ensuring "mandatory measures that must be taken to 'correctly' store and process personal data." A comprehensive risk assessment framework is essential for mitigating these vulnerabilities.

Unauthorized access and cyber threats

Unauthorized access and cyber threats represent significant risks to personal data across sectors. Abomhara and Køien (2015) note that the "number of threats is rising daily, and attacks have been on the increase in both number and complexity." Cybercriminals exploit vulnerabilities, often utilizing "design faults" in web applications (Razzaq, Hur, Ahmad, & Masood, 2013). This reality emphasizes the need for robust security measures. Institutions should implement strategies like intrusion detection systems and employee training. As the literature suggests, "understanding attackers' motives and capabilities is important for an organization to prevent potential damage" (Abomhara & Køien, 2015, p. 81).

Data loss and corruption

Data loss and corruption represent critical risks in modern data management systems, affecting data integrity and availability. Data loss refers to the unintentional destruction or disappearance of data due to hardware failures, software bugs, or cyber-attacks, while corruption alters data, rendering it unusable or inaccurate. In data center networks, packet corruption can lead to significant packet losses and degrade application performance, with stable rates remaining uncorrelated with link utilization (Zhuo et al., 2017). To mitigate these risks, techniques like Fast Integrity VERification (FIVER) help minimize verification costs (Arslan & Alhussen, 2021). Studies also stress the importance of robust fallback strategies for managing ICT errors (Klaes et al., 2023)

To prevent future data loss, set up a reliable backup system and automate backups to avoid human error. Implement data versioning to maintain multiple versions of your files, which helps restore previous versions if corruption occurs. Strengthen your cybersecurity to protect against ransomware and other cyber threats. In case of data loss or corruption, follow practical steps to restore your system with minimal impact. Many people believe they are backing up their data but often don't perform drills to ensure the data can be restored properly. Therefore, I highly recommend that churches or nonprofits conduct regular data recovery drills, either biannually or annually.

Common Sources of Risks

Ministries must proactively address various sources of risk to ensure data protection and privacy. Firstly, they need to mitigate internal threats, such as employee negligence. Secondly, they must defend against external threats like cyberattacks. Lastly, they should manage vulnerabilities from third-party vendors and partnerships. Each of these challenges significantly impacts the safeguarding of sensitive information.

Internal threats (e.g., employee negligence)

Employee negligence is a significant internal threat to information security, often arising from non-malicious actions that compromise institutional assets. Brown (2020) notes that "non-malicious insiders are a danger to an organization’s stability because their negligence or carelessness towards policies can lead to unintentional breaches" (p. 2). This negligence typically stems from a lack of understanding or awareness of security policies due to insufficient training

(Olabanji, 2019). Hills and Anjali (2017) stress the need for a security-aware culture, stating that "the threat posed by a malevolent insider can be even more challenging" (p. 2). Effective governance must include comprehensive training to mitigate insider threats..

External threats (e.g., cyberattacks)

Cyberattacks present a significant external threat to organizations, characterized by evolving tactics and increasing sophistication. Bendovschi (2015) states that cybercrime continually develops new attack types and tools, enabling attackers to penetrate complex environments and remain untraceable (p. 24). Attributing cyberattacks is nuanced, requiring both technical and non-technical skills to reduce uncertainty (Rid & Buchanan, 2015). Effective public attribution can achieve strategic goals like norm-setting and deterrence but must be managed carefully to avoid unintended consequences (Egloff & Smeets, 2023). As threats grow, organizations must adopt comprehensive security countermeasures to protect sensitive information.

Third-party vendors and partnerships

Vendors and partnerships pose significant risks due to informational asymmetries, where one party has better information, potentially leading to opportunism or misaligned incentives (Akerlof, 1970; Williamson, 2008). Suppliers might overstate their capabilities or underreport compliance gaps, while partners could conceal conflicting interests. Relying on a single supplier can create vulnerabilities, such as supply chain disruptions (Poret, 2014). Misconduct by a partner can damage an organization's credibility, leading to reputational spillover (Baur & Schmitz, 2012). Effective risk mitigation requires robust due diligence, clear contracts, and ongoing monitoring for alignment and accountability.

These external entities often have access to sensitive data and systems, making them targets for cyberattacks. Inadequate security measures can lead to data breaches and unauthorized access. Managing a large number of external relationships can be overwhelming, as each brings unique risks, increasing complexity. Churches and nonprofits often struggle to maintain visibility into their partners' operations and risk management practices, hindering effective risk assessment and mitigation. Ensuring compliance with relevant regulations and standards can be difficult, especially with partners across different regions and industries. Churches and nonprofits fail to continuously monitor their partners for compliance and risk management, allowing new risks to

emerge unnoticed. Heavy reliance on a single supplier can disrupt operations and supply chains if the supplier fails to deliver. Misconduct or failures by an external partner can damage the institute's reputation, causing long-term negative effects on trust and credibility. Financial instability or failure of a supplier can impact the establishment's financial health, including risks related to non-delivery of goods or services and potential financial losses.

Addressing these challenges requires a comprehensive risk management strategy, including thorough due diligence, clear contractual agreements, continuous monitoring, and effective communication with partners.

Communicating Data Protection Efforts

To maintain stakeholder trust, ministries must clearly communicate their data protection efforts. Firstly, they prioritize transparency, ensuring stakeholders understand how they manage information. Secondly, they provide regular updates to reinforce this commitment, assuring stakeholders that responsible parties actively uphold data protection measures. Lastly, they demonstrate dedication to safeguarding sensitive information and fostering trust through consistent communication.

Transparency in data practices

Effective communication about data protection enhances transparency and trust among data subjects. The General Data Protection Regulation (GDPR) mandates that data processors provide clear information regarding processing activities (Spagnuelo, Ferreira, & Lenzini, 2019). Transparency-enhancing design patterns, such as layered notices and FAQs, improve the clarity of information (Rossi & Lenzini, 2020). By embedding these measures into data processing, ministries enhance accountability and promote ethical data practices.

Regular updates and reports to stakeholders

Communicating data protection efforts is crucial for maintaining stakeholder trust and ensuring compliance. Regular updates and reports play a pivotal role in this process. Diers-Lawson and Symons (2021) emphasize proactive relationship building and strategic communication in managing data breaches, noting that ongoing crisis capacity building enhances resilience. Gitari (2023) highlights that transparency and engagement improve trust and compliance. Together, these studies underscore the importance of regular, transparent communication as part of effective data protection strategies.

Financial Risk Management

Financial risk management is vital for churches and nonprofits to ensure compliance and accountability. Firstly, they must review relevant laws, such as the GDPR and the Health Insurance Portability and Accountability Act (HIPAA), and discuss their implications. Secondly, they should establish accountability by designating a data protection officer and defining roles. Lastly, adhering to regulations safeguards financial integrity and maintains stakeholder trust.

Regulatory Compliance

Churches and nonprofits must navigate regulatory compliance to protect sensitive data and maintain stakeholder trust. Firstly, they need to understand key requirements of relevant laws, such as GDPR and HIPAA. Secondly, they should discuss the implications of these laws for their ministries. Lastly, they must emphasize the necessity of adhering to legal standards to safeguard personal information and ensure institutional integrity.

Overview of relevant laws

Non-Governmental Organizations (NGOs) navigate complex regulations to manage financial risks, particularly under laws like GDPR and HIPAA. GDPR mandates explicit consent for data processing and robust security protocols, while HIPAA requires risk analyses and safeguards for electronic protected health information (ePHI). Luna (2018) emphasizes that effective risk management maintains data integrity, confidentiality, and availability through defined roles and policies. Gade (2020) underscores the need for appropriate risk assessment methodologies to address vulnerabilities. Integrating these requirements helps NGOs safeguard sensitive information and ensure operational resilience.

Implications for churches and nonprofits

Organizations, including churches and nonprofits, face significant challenges in financial risk management, especially regarding regulatory compliance. Effective financial risk management safeguards assets while ensuring adherence to standards to avoid legal repercussions and maintain public trust. Zietlow, Hankin, and Seidner (2007) stress the need for comprehensive financial policies that address accountability and compliance, crucial for mitigating risks (p. 147). Seaman and Young (2010) highlight that internal controls and governance structures enhance financial stability and compliance (p. 75). These measures are essential for navigating complex regulatory environments and sustaining operations effectively.

Establishing Accountability

Establishing accountability is critical for effective data protection. Ministries must designate a data protection officer or team. They should set clear roles and responsibilities to ensure comprehensive oversight. They also need to manage data security measures effectively.

Designating a data protection officer or team

Ministries face considerable financial risks, particularly concerning data protection and accountability. Appointing a Data Protection Officer (DPO) is a crucial strategy for mitigating these risks. The DPO ensures compliance with data protection laws, conducts risk assessments, and implements policies to safeguard sensitive information. This role is vital for maintaining transparency and trust with stakeholders and preventing financial losses from data breaches (Lambert, 2019). Furthermore, the accountability principle in data protection emphasizes the need for internal mechanisms to demonstrate compliance, essential for effective financial risk management (Alhadeff, Van Alsenoy, & Dumortier, 2012). Appointing a DPO enhances these practices and ensures robust data protection.

Setting clear roles and responsibilities

Enhancing financial risk management requires NGOs to establish clear roles and responsibilities for accountability. Ribstein (2006) notes that accountability in corporate governance involves defining explicit duties for managers to act in stakeholders' best interests and adhere to ethical standards. Khotami (2017) emphasizes that good governance demands transparency and clear delineation of responsibilities to maintain public trust. By defining specific roles, NGOs can mitigate financial risks, improve decision-making, and foster a culture of accountability and transparency, thereby strengthening their governance framework and resource management.

Operational Risk Management

Operational Risk Management focuses on protecting sensitive data by identifying vulnerabilities and assessing data protection needs. This process includes conducting thorough risk assessments to evaluate current measures. It also involves understanding stakeholder perspectives to address their concerns effectively. Engaging stakeholders and educating staff through training programs fosters a culture of privacy, ensuring robust data protection within the ministry.

Assessing Data Protection Needs

In the section on **Assessing Data Protection Needs**, we will design and conduct the risk assessment annually. Next, we will identify key sensitive data to ensure proper protection. Following that, we will evaluate current data protection measures to determine their effectiveness. Finally, we will analyze potential vulnerabilities to strengthen our security posture.

Conducting a Risk Assessment

A risk assessment is vital for operational risk management in NGOs, helping to identify potential threats and vulnerabilities that could hinder their objectives. This assessment systematically evaluates the likelihood and impact of various risks, including financial, legal, security, and reputational factors. NGOs should consider their operational context, including local capacities (Trivunovic, Johnsøn, & Mathisen, 2011). Additionally, they must account for internal and external factors, such as compliance with local laws and corruption risks (Stoddard, Haver, & Czwarno, 2016). Thorough risk assessments enable NGOs to develop tailored mitigation strategies, enhancing resilience and program sustainability.

Identifying sensitive data

NGOs face significant operational risks in managing sensitive data. The rise of sophisticated risk management frameworks among international NGOs underscores the need to safeguard this information. These frameworks, adapted from private sector practices, utilize tools like risk registers and matrices to systematically assess and mitigate risks (Stoddard, Haver, & Czwarno, 2016). Despite advancements, gaps in information security and legal compliance persist, highlighting the need for stronger policies to protect sensitive data from breaches (Stoddard et al., 2016). Addressing these vulnerabilities is crucial for maintaining the integrity and effectiveness of humanitarian operations.

Evaluating current data protection measures

Organizations must strengthen data protection measures to enhance their risk management framework and ensure long-term sustainability. In Migori County, Kenya, significant challenges exist, particularly regarding data protection gaps that jeopardize sensitive information. Opiyo (2018) emphasizes that while funding mechanisms are in place, transparency and accountability are essential for efficient resource allocation and donor retention. This situation highlights the urgent need to evaluate and improve data protection measures to mitigate risks effectively.

Analyzing potential vulnerabilities

Addressing vulnerabilities in operational risk management frameworks is critical for effective humanitarian response. Stoddard, Haver, and Czwarno (2016) identify gaps in current practices, including insufficient focus on information security and legal compliance. These vulnerabilities can lead to data breaches and fraud, undermining operational integrity. Developing comprehensive risk management policies is essential to mitigate these risks and enhance organizational resilience.

Stakeholder Perspectives

Understanding stakeholder expectations is crucial for effective data protection. To address this, we will engage with stakeholders to assess their data protection concerns. This collaborative approach will help us tailor our strategies and enhance trust.

Importance of understanding stakeholder expectations

Understanding stakeholder expectations is crucial for operational risk management in non-governmental organizations. Stoddard, Haver, and Czwarno (2016) emphasize that donors significantly influence the risks NGOs are willing to assume, affecting decisions on program locations, security measures, and legal compliance. Donors' focus on fiduciary risk and zero tolerance for corruption leads NGOs to adopt stringent controls, necessitating a balance between these expectations and operational goals to maintain donor trust and achieve resilience.

Engaging with stakeholders to assess their data protection concerns

Engaging stakeholders to assess data protection concerns is vital for operational risk management in NGOs. Trivunovic, Johnsøn, and Mathisen (2011) highlight the importance of incorporating stakeholder feedback into corruption risk management systems. By involving stakeholders, institutes can identify specific vulnerabilities and tailor their strategies, enhancing transparency, accountability, and trust. This collaborative approach ultimately strengthens the integrity and effectiveness of operations.

Training and Awareness Programs

Educating staff on data protection policies is essential for ensuring compliance and safeguarding sensitive information. To achieve this, we will focus on creating a culture of privacy where all employees understand and adhere to data protection practices. By implementing comprehensive training and awareness programs, we can enhance overall data security and foster a proactive approach to privacy.

Educating staff on data protection policies

Educating staff about data protection policies is critical for operational risk management in NGOs. Talbot and Jakeman (2011) emphasize integrating security risk management principles into organizational practices to safeguard sensitive information. Comprehensive training equips staff to identify and mitigate potential risks, enhancing resilience against data breaches and fostering a culture of security awareness and accountability. Robust education programs align with best practices and contribute to the overall integrity of operations.

Creating a culture of privacy within the organization

Creating a culture of privacy is essential for operational risk management in NGOs. Stoddard, Haver, and Czwarno (2016) emphasize integrating privacy considerations into practices to mitigate information security risks. Fostering this culture ensures staff adhere to data protection policies, reducing data breaches and unauthorized access. This proactive approach enhances resilience against security threats and builds trust with stakeholders, aligning with best practices in risk management and contributing to operational integrity.

Institutional Risk Management

The institutionalization of risk management actively integrates practices into an institutes's core operations, culture, and decision-making. This process involves creating formal policies and frameworks for risk assessment, fostering a risk-aware culture where employees understand their roles, and providing ongoing training to equip staff with necessary skills. Regularly reviewing and improving these practices, while aligning them with strategic goals, enhances resilience and protects assets.

In this context, we will now focus on developing a Data Protection Strategy. This strategy will prioritize objectives and tasks, ensuring effective resource allocation and success measurement as we implement data protection and privacy measures. Following this, we will establish an Incident Response Plan to address potential data breaches. This plan will include disaster recovery procedures and communication strategies to minimize impact and keep stakeholders informed. Together, these elements create a cohesive approach to managing data protection and maintaining trust.

Developing a Data Protection Strategy

Developing a data protection strategy is crucial for NGOs to manage institutional risk effectively. Kassen (2018) underscores the importance of aligning data protection strategies with

institutional values and mission to ensure comprehensive risk management. By adopting open data principles and engaging stakeholders, NGOs can identify potential vulnerabilities and implement robust data protection measures. This approach not only enhances transparency and accountability but also fosters trust and cooperation among stakeholders. Integrating stakeholder perspectives into data protection strategies helps NGOs address challenges and develop policies that safeguard sensitive information while promoting institutional resilience.

Setting objectives for data protection

Developing a data protection strategy is essential for institutions to manage institutional risk effectively. Stoddard, Haver, and Czwarno (2016) emphasize the importance of integrating data protection measures into practices to mitigate information security risks. By aligning clear objectives with institutional values, NGOs can enhance their resilience against data breaches and unauthorized access. This proactive approach safeguards critical data and fosters trust among stakeholders, ensuring the integrity and effectiveness of operations.

Aligning strategies with organizational values and mission

Aligning strategies with organizational values and mission is crucial for institutional risk management in non-governmental organizations. Tugyetwena (2023) highlights that robust governance structures and diversified funding strategies are essential for sustainability. This alignment enhances legitimacy and credibility among stakeholders, fostering trust and strong partnerships vital for securing funding and achieving long-term goals. Integrating values into strategic planning strengthens governance and contributes to the overall resilience of NGOs.

Incident Response Plan

Developing an incident response plan is vital for managing institutional risk, particularly concerning data breaches. Institutions should establish a comprehensive strategy to contain and mitigate impacts while implementing long-term prevention measures. Clear communication plans are essential for maintaining transparency and trust with stakeholders during these events, outlining protocols for notifying affected parties, providing updates, and offering guidance. Proactively addressing data breaches enhances reputation and resilience against future incidents.

Developing a response strategy for data breaches

NGOs must prioritize institutional risk management by creating robust response strategies for data breaches. Diers-Lawson and Symons (2021) stress the importance of proactive

stakeholder relationship management and strategic communication in building crisis capacity. Their research indicates that NGOs should focus on pre-crisis relationship building to mitigate breach impacts. Effective crisis communication must address both technical aspects and reputational damage. By fostering trust-based relationships and implementing comprehensive plans, NGOs can enhance resilience and maintain stakeholder confidence during data security incidents.

Communication plans for stakeholders in the event of a breach

Communication plans are crucial for NGOs in managing institutional risk during data breaches. Leopkey and Parent (2007) underscore the importance of stakeholder engagement and strategic communication for large-scale events. NGOs should develop comprehensive strategies that address stakeholders' concerns and provide clear, timely information during a breach. By prioritizing transparent communication and relationship management, NGOs can mitigate the negative impacts of data breaches and maintain trust among stakeholders.

Conclusion

In conclusion, this paper emphasizes the vital role of proactive data protection and privacy measures in preserving trust and integrity among stakeholders. We have examined various dimensions of reputational, financial, and operational risk management, incorporating them extensively into institutional risk management. This highlights the necessity for transparency, regulatory compliance, and strong accountability frameworks. By thoroughly understanding and addressing data protection and privacy risks, institutions can cultivate a robust culture of privacy that aligns with their core values of transparency and integrity.

Moreover, the commitment to these essential practices not only safeguards sensitive information but also fortifies stakeholder trust and confidence. Adhering to regulations such as GDPR and HIPAA is non-negotiable, as is establishing clear accountability through dedicated roles like a Data Protection Officer. Engaging stakeholders through proactive communication is crucial for building trust and enhancing transparency. Continuous training and education further equip institutions to foster a culture of privacy.

Ultimately, by prioritizing these comprehensive strategies, institutions not only protect critical data but also enhance their overall resilience and effectiveness, ensuring they meet both current and future challenges with confidence.

References

Abomhara, M., & Køien, G. M. (2015, September 14). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security, 4, 65-88.

Adams, C., & Abhayawansa, S. (2022). Connecting the COVID-19 pandemic, environmental, social and governance (ESG) investing and calls for 'harmonisation'of sustainability reporting. Critical Perspectives on Accounting, 82, 102309.

Adeyemi, O. A., & Adeyinka, O. A. (2015). Effective management in church organizations. Journal of Management and Strategy, 6(1), 1-12 doi: 10.5430/jms.v6n1p1.

Akerlof, G. F. (1970). The market for 'lemons': quality uncertainty and the market mechanism. Market Failure or Success, 66.

Alhadeff, J., Van Alsenoy, B., & Dumortier, J. (2012). The accountability principle in data protection regulation: origin, development and future directions. In Managing privacy through accountability, 49-82.

Alhawari, S., Karadsheh, L., Talet, A., & Mansour, E. (2012). Knowledge-based risk management framework for information technology project. International Journal of Information Management, 32(1), 50-65.

Amankwah-Amoah, J., Khan, Z., Wood, G., & Knight. (2021). COVID-19 and digitalization: The great acceleration. Journal of Business Research, 136, 602-611.

Appiah, R., & Blankson, I. (2022). Occupational Health and Safety Management Practices and Employee Safety Behavior: Evidence from Accra Technical University, Ghana. The International Journal of Humanities & Social Studies, 10(3).

Ariawan, S., & Simorangkir, J. (2021). Understanding the Pattern of Sowing-Reaping in Christianity: Efforts to Redesign the Model of Christian Education in Schools Facing the Aftermath of the Covid-19 Pandemic. the International Journal of Education, Theology, and Humanities. , 1(1), 1-7.

Arslan, E., & Alhussen, A. (2021). A Low-Overhead Integrity Verification for Big Data Transfers. Journal of Parallel and Distributed Computing(152), 33-44.

Baur, D., & Schmitz, H. P. (2012). Corporations and NGOs: When Accountability Leads to Co-optation. Journal of Business Ethics(106), 9-21.

Beaumont, S. (2019). How to Lead when You Don't Know where You're Going: Leading in a Liminal Season. Rowman & Littlefield.

Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. Procedia Economics and Finance(28), 24-31.

Birkbeck, C., & Wilkin, C. (2020). The Impact of COVID-19 on Nonprofit Fundraising: An Analysis of Giving Tuesday Data. Nonprofit and Voluntary Sector Quarterly, 49(5), 1011-1022.

Block, P. (1993). Stewardship: Choosing Service Over Self-Interest.

Blume, P. (2010). Data Protection and Privacy – Basic Concepts in a Changing World. Scandinavian Studies In Law, 152-163.

Bowman, S. (2022). A Pneumatological Theology and Christological Philosophy of Church Conflict for the Post-Pandemic Western Church to Outlive, Outlast, and Outlove. (Doctoral dissertation, Southeastern University).

Bowrin, A. (2004). Internal control in Trinidad and Tobago religious organizations. Accounting, Auditing & Accountability Journal, 17(1), 121-152.

Branson, M. L. (2010). Strategic Planning and Discernment in Christian Ministry Organizations: Complementary or Contradictory Approaches? Christian Higher Education, 9(3-4), 249-261.

Brinkman, J. (2018). Practicing discernment in ministry: A theological framework. Journal of Spiritual Formation & Soul Care, 11(1), 5-20.

Brown, A. (2020). Why Are Non-malicious Employees Non-Compliant: Guidance for Identifying Employee Negligence and Implementing Information Security Policies to Reduce Employees Inadvertently Becoming Insider Threats. Master's thesis.

Bryson, J. M. (2018). Strategic planning for public and nonprofit organizations: A guide to strengthening and sustaining organizational achievement. John Wiley & Sons.

Cha, S. C., & Yeh, K. H. (2018, September 28). A data-driven security risk assessment scheme for personal data protection. IEEE Access,, 6, 50510-50517.

Chillakuri, B., & Mahanandia, R. (2018). Generation Z entering the workforce: the need for sustainable strategies in maximizing their talent. Human Resource Management International Digest, 26(4), 34-38.

Costello, S. (2022). Dynamics of Discernment: A Guide to Good Decision-Making (Vol. 13). Wipf and Stock Publishers.

Crouch, A., Keilhacker, K., & Blanchard, D. (2020). Leading beyond the blizzard: Why every organization is now a startup. Praxis Labs.

de Andrade, N. (2011). Data protection, privacy and identity: distinguishing concepts and articulating rights. Springer Berlin Heidelberg., 90-107.

Diers-Lawson, A., & Symons, A. (2021). Building crisis capacity with data breaches: the role of stakeholder relationship management and strategic communication. Corporate Communications: An International Journal.(ISSN 1356-3289 DOI: https://doi.org/10.1108/CCIJ-02-2021-0024).

Dokuchaev, V. A., Maklachkova, V. V., & Statev, V. Y. (2020). Classification of personal data security threats in information systems. T-Comm-Телекоммуникации и Транспорт, 14(1), 56-60.

Eccles, R. (2004). Hopes and fears for financial reporting and corporate governance. Balance Sheet, 12(3), 8-13.

Egloff, F. J., & Smeets, M. (2023). Publicly attributing cyber attacks: a framework. Journal of Strategic Studies, 46(3), 502-533.

Ferris, J. M., Fletcher, E. L., & Fernhaber, S. (2015). Transforming the nonprofit sector: Evidence-based ideas, models, and strategies for nonprofit leaders. John Wiley & Sons.

Gade, R. B. (2020). Data Governance and Risk Management: Mitigating Data-Related Threats. Advances in Computer Sciences, 3.

Gellert, R., & Gutwirth, S. (2013). The Legal Construction of Privacy and Data Protection. Computer Law & Security Review (CLSR), 29, 522-530.

Gitari, E. K. (2023). Data Protection and Experience of Stakeholders at the University of Nairobi. ((Doctoral dissertation, University of Nairobi)).

Hai, T., Van, Q., & Thi Tuyet, M. (2021). Digital transformation: Opportunities and challenges for leaders in the emerging countries in response to COVID-19 pandemic. Emerging Science Journal, 5(1), 21-36.

Hamilton, A. (2022). Theology for Psychology and Counseling: An Invitation to Holistic Christian Practice.

Hills, M., & Anjali, A. (2017). A human factors contribution to countering insider threats: Practical prospects from a novel approach to warning and avoiding. Security Journal, 30(1), 142-152.

Hinchliff, M. (1996). The puzzle of change. Philosophical perspectives(10), 119-136.

Homer, S., & Khor, K. (2022). Exploring the perceptions of Malaysian Gen Z towards the impact of COVID-19 on sustainable development. Environmental Science and Pollution Research, 29(57), 85700-85716. .

Hong, P., & Kwon, I. (2019). Best practices of process management in nonprofit organizations: A case study of a Christian nonprofit organization. Journal of Nonprofit & Public Sector Marketing, 31(2), 151-166. doi: 10.1080/10495142.2018.1513845.

Kassen, M. (2018). Adopting and managing open data: Stakeholder perspectives, challenges and policy recommendations. Aslib Journal of Information Management, 70(5), 518-537.

Khotami, M. (2017). The concept of accountability in good governance. In International Conference on Democracy. Accountability and Governance, ICODAG, 30-33.

Klaes, M., Zwartscholten, J., Narayan, A., Lehnhoff, S., & Rehtanz, C. (2023, February 16). Impact of ict latency, data loss and data corruption on active distribution network control. IEEE Access(11), 14693-14701.

Kovner, A. (2014). Evidence-based management: Implications for nonprofit organizations. . Nonprofit Management and Leadership, 24(3), 417-424.

Lambert, P. (2019). The Data Protection Officer: Profession, Rules, and Role. CRC Press.

Leopkey, R., & Parent, M. (2007). Risk management issues in large-scale sporting events: A stakeholder perspective. North American Society for Sport Management Conference (NASSM 2007).

Li, K., & Griffin, M. (2022). Prevention-focused leadership and well-being during the pandemic: mediation by role clarity and workload. . Leadership & Organization Development Journal, (ahead-of-print).

Luna, R. B. (2018). A Framework for Evaluation of Risk Management Models for HIPAA Compliance for Electronic Personal Health Information used by Small and Medium Businesses using Cloud Technologies. (Master's thesis, East Carolina University).

Mahapatra, G., Bhullar, N., & Gupta, P. (2022). Gen Z: an emerging phenomenon. NHRD Network Journal, 15(2), 246-256.

Martin, R. (2019). When Money Goes on Mission: Fundraising and Giving in the 21st Century. Moody Publishers.

Mellon, J., & Kroth, M. (2013). Experiences That Enable One to Become an Expert Strategic Thinker. . Journal of Adult Education, 42(2), 70-79.

Mesch, D., Osili, U., Skidmore, T., & Bergdoll, J. (2020). COVID-19, generosity, and gender: How giving changed during the early months of a global pandemic. Women’s Philanthropy Institute, Indianapolis,.

Miller, D. (2007). Financial Management for Christian Organizations: A Theological Perspective. Journal of Markets & Morality.

Mitchel, P. (2021, January 13). Wisdom during the Pandemic. Christianity Today, pp. https://www.christianitytoday.com/scot-mcknight/2021/january/wisdom-during-pandemic.htmlhttps://www.christianitytoday.com/ct/2021/january-web-only/pandemic-accelerated-digital-transformation-churches.html.

Nehari-Talet, A., Karadsheh, L., Alhawari, S., & Hunaiti, H. (2021). The Importance of Knowledge-Based Risk Processes to Risk Analysis. International Journal of Knowledge Management (IJKM), 17(1), 33-51.

North Whitehead, A. (1929). Process and reality: an essay in Cosmology.

Olabanji, O. (2019). Exploring the application of information security governance in mitigating insider negligence threats: A qualitative analysis. Doctoral dissertation.

Opiyo, M. O. (2018). Risk management practices and financial sustainability of non-governmental organizations in Migori County, Kenya. University of Nairobi.

Poret, S. (2014). Corporate-NGO partnerships in CSR activities: why and how?

Porter, M. E. (1996). The benefits of strategic planning. California management review, 39(4), 8-21.

Poullet. (2010). 9.

Razzaq, A., Hur, A., Ahmad, H. F., & Masood, M. (2013, March). Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. . In 2013 IEEE Eleventh International Symposium on Autonomous Decentralize, 1-6.

Ribstein, L. E. (2006). Accountability and Responsibility in Corporate Governance. Notre Dame Law Review, 81(4), 1432-1466.

Rid, T., & Buchanan, B. (2015). Attributing cyber-attacks. Journal of Strategic Studies, 38(1-2), 4-37.

Rivera-Santos, M., Rufín, C., & Wassmer, U. (2017). Alliances between firms and non-profits: A multiple and behavioural agency approach. Journal of Management Studies, 54(6), 854-875.

Rossi, A., & Lenzini, G. (2020). Transparency by design in data-informed research: A collection of information design patterns. Computer Law & Security Review, 37,(37), 105402.

Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber risk in health facilities: A systematic literature review. . Sustainability, 12 (17), 7002.

Seaman, B. A., & Young, D. R. (2010). Introduction: The Frontiers of Economics and Nonprofit Management Research. In Handbook of Research on Nonprofit Economics and Management. Edward Elgar Publishing.

Settembre-Blundo, D., González-Sánchez, R., Medina-Salgado, S., & García-Muiña, F. (2021). Flexibility and resilience in corporate decision making: a new sustainability-based risk management system in uncertain times. Global Journal of Flexible Systems, 22 (Suppl 2), 107-132.

Sheikhi, R., Seyedin, H., Qanizadeh, G., & Jahangiri, K. (2021). Role of religious institutions in disaster risk management: A systematic review. Disaster medicine and public health preparedness, 15(2), 239-254.

Solove, D. J. (2024). Data is what data does: regulating based on harm and risk instead of sensitive data. Northwestern University Law Review, 118, 1081 - 1138.

Spagnuelo, D., Ferreira, A., & Lenzini, G. (2019, March). Accomplishing Transparency within the General Data Protection Regulation. In ICISSP, 114-125.

Stoddard, A., Haver, K., & Czwarno, M. (2016). NGOs and Risk.

Talbot, J., & Jakeman, M. (2011). Security risk management body of knowledge. Wiley.

Trivunovic, M., Johnsøn, J., & Mathisen, H. (2011). Developing an NGO corruption risk management system: Considerations for donors. (U4 Issue).

Tugyetwena, M. (2023). A literature review of the relationship between governance, funding strategy and sustainability of non-government organizations. International NGO Journal, 18(2), 10-19.

Van Tiem, D., Moseley, J., & Dessinger, J. (2012). Fundamentals of performance improvement: Optimizing results through people, process, and organizations. John Wiley & Sons.

Waldman, D. A., & Von Glinow, M. (2004). Building Organizational Resilience. Journal of Management, 30(6), 702-718.

Williamson, O. E. (2008). The economic institutions of capitalism. The Political Economy Reader: Markets as Institutions. 27.

World Health Organization. (2021). COVID-19 strategic preparedness and response plan: operational planning guideline: 1 February 2021 to 31 January 2022 (No. WHO/WHE/2021.03). World Health Organization.

Zhuo, D., Ghobadi, M., Mahajan, R., Förster, K. T., Krishnamurthy, A., & Anderson, T. (2017, August). Understanding and mitigating packet corruption in data center networks. In Proceedings of the Conference of the ACM Special Interest Group on Data Communication, 362-375.

Zietlow, J., Hankin, J. A., Seidner, A., & O'Brien, T. (2018). Financial management for nonprofit organizations: Policies and practices. John Wiley & Sons.

Abstract

This paper examines reputational, financial, and operational risk management for churches and nonprofits, focusing on safeguarding personal information to maintain stakeholder trust. It highlights strategies for effective communication about data protection efforts and establishing accountability measures. By addressing these risks, organizations can foster a culture of privacy and align their missions with transparency and integrity principles. The paper emphasizes the need for proactive data protection, regulatory compliance, and incident response plans to mitigate data breach impacts. Through analysis and practical recommendations, it aims to enhance organizational resilience and maintain stakeholder confidence in the digital age.

Keywords: Data protection, privacy, risk management, churches, nonprofits, stakeholder trust, regulatory compliance, incident response.

About the Author

Trevor Lui, Ed.D., serves as the Deputy CEO of Global Trust Partners (www.gtp.org). He trusts that God provides enough and embraces his role as a steward, using his consulting experience to serve others. Trevor earned his Ed.D. in Knowledge Management from The University of Hong Kong (HKU) and teaches at both the Faculty of Education and the Business School at HKU. He resides in Hong Kong.