CARTERS
Integrated Practice, Proactive Advice

*The 2024 Carters Annual*
*Charity & Not-for-Profit Law Webinar*
**Thursday, November 14, 2024**

# IT and Data Management: Board Governance Issues to Consider

**By Esther Shainblum, B.A., LL.B., LL.M., CRM &**
**Cameron Axford, B.A., J.D.**

eshainblum@carters.ca
caxford@carters.ca
1-877-942-0001

CARTERS
Integrated Practice, Proactive Advice

# Carters Annual *Charity & Not-for-Profit Law* Webinar

November 14, 2024

# IT and Data Management: Board Governance Issues to Consider

**By Esther Shainblum & Cameron Axford**



**Carters Professional Corporation**
Lawyers & Trademark Agents

Orangeville • Ottawa • Toronto
**www.carters.ca** **Toll Free: 1-877-942-0001**

## Overview of Presentation

- A Setting the Stage
- B Understanding the Risk
- C The Importance of Governance in Effective IT and Data Management
- D IT Governance Responsibilities
- E Practical Steps for Directors and Officers to Take in Managing the Risks
- F Key Takeaways

## A. Setting the Stage

- Charities and not-for-profits (collectively "NFP Corporations") depend on their information technology ("IT") infrastructure to manage and administer their overall operations
- As NFP Corporations become increasingly dependent on their IT infrastructure, the greater the risk to the NFP Corporation if there is an IT failure or interruption, and the greater portion of its budget must be spent on IT infrastructure
- Directors must consider how reliant the NFP Corporation is on the IT infrastructure, what possible risks may exist and what strategies are necessary to address those risks
- Failure to properly manage an NFP Corporation's IT infrastructure and the associated risks could expose its board of directors to potential liability
- This presentation reviews board governance issues as they relate to IT and data management
- First, though, need to understand the risks involved and basic governance principles



## B. Understanding the Risk

- Like their for-profit counterparts, NFP Corporations are increasingly reliant on IT infrastructure for core operational functions, such as managing their activities and operations, overseeing their employees, serving their clients, engaging with their donors, paying their vendors and suppliers and maintaining their books and records
- NFP Corporations are also active in the digital/online landscape, including:
  - Public facing websites
  - Online presence/social media
  - Online donation forms
  - Cloud-based platforms for core business processes, such as video conferencing, donor management and payment processing (e.g. Zoom, Blackbaud, Stripe)

## 1. Why Effective IT Governance Matters to NFP Corporations

- Safeguard Donor Trust
  - Protecting donor data ensures trust, strengthens relationships, and encourages continued support
  - Data breaches can damage reputation and erode public confidence
- Enhance Operational Efficiency
  - Effective data management streamlines operations, reduces redundancy, and facilitates informed decision-making, allowing resources to be allocated more effectively
- Mitigate Security Risks
  - Proactive IT management helps identify and address vulnerabilities, reducing the risk of cyber threats, privacy and data breaches, business interruption and financial loss
- Support Mission Fulfillment
  - Clear, organized data supports transparent reporting and strategic planning, helping NFP Corporations to measure impact, set goals, and fulfill their mission




## 2. IT Related Risks that Directors Need to be Aware of:

a) Cybersecurity Threats

- In 2024 Canadian organizations paid an average cost of $6.32 million per data breach
- The average ransom paid in ransomwear attacks in Canada has increased significantly, more than $1.130 million, an increase of nearly 150% in two years
- 58% of affected mid-market companies say that it took more than a month to recover from an attack, 24% said that it took longer than four months, up from 17% in 2021

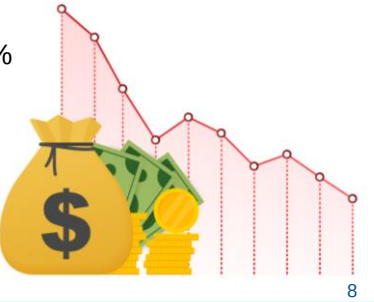
b) Business Interruption

- The more reliance an NFP Corporation places on its IT infrastructure, the greater the risk that any failure of the IT infrastructure will damage its operations
- IT related business interruption can be caused by cyber incidents, equipment or machinery failure, a fire, flood or other disaster that causes damage to IT infrastructure, loss of records or backups, human error, a power failure or a supplier's IT failure
- Any of these could hamper or even shut down an NFP Corporation's operations
- This summer's Crowdstrike failure caused a worldwide shut down of various industries and left people without access to many services, from finance to healthcare to travel
- NFP Corporations that rely on cloud service providers for e-commerce and other core functions could experience a business interruption if that provider goes down



c) Cost Overruns and Revenue Losses

- Directors of NFP Corporations, especially charities, have a fiduciary duty to act in the best interests of the corporation and, in the case of charities, to safeguard charitable assets
- IT investments can be so large and can impact so many aspects of an organization that they can pose a risk to NFP Corporations
- In 2020, McKinsey & Company found that 17% of large IT projects go so badly, they threaten the very existence of the company
- Half of large IT projects exceed budgets and timelines, often delivering only half of expected value
- Research shows large IT projects can go over budget by 45% and fall short on benefits by 56%
- Projects often struggle due to unclear objectives, shifting requirements, team skill gaps, and reactive planning



## C. The Importance of Governance in Effective It and Data Management

### 1. What is Good Governance?

- The law and the public look to the NFP Corporation's governing body, i.e., the board of directors, to put in place the rules, processes and structures used to direct and manage the NFP Corporation's operations and activities
- Governance includes having clear lines of accountability and responsibility and ensuring that the NFP Corporation acts in accordance with the law
- The goal of good governance is to ensure the effectiveness, credibility and sustainability of the NFP Corporation
- Risk oversight is increasingly seen as a key competence of boards of directors
- Effective management of the NFP Corporation's IT infrastructure – including appropriate risk management strategies – is an essential aspect of corporate governance



### 2. The Statutory Duties of Directors and Officers of NFP Corporations

### a) Statutory Duty to Manage the Corporation

- Under both the *Canada Not-for-Profit Corporations Act* ("CNCA") and the Ontario *Not-for-Profit Corporations Act* ("ONCA"), the directors have a duty to "manage or supervise the management of the activities and affairs of [the] corporation"
  - To fulfill this duty, directors must ensure:
    - The purposes of the NFP Corporation are properly carried out and activities undertaken fit within those purposes
    - The NFP Corporation is financially stable
    - Proper management of corporate assets and infrastructure
    - Proper hiring, training, and supervision of management, staff and volunteers
    - The overall operating integrity of the corporation
  - Does not involve interference with day to day operations by management

**b) Statutory Fiduciary Duty**

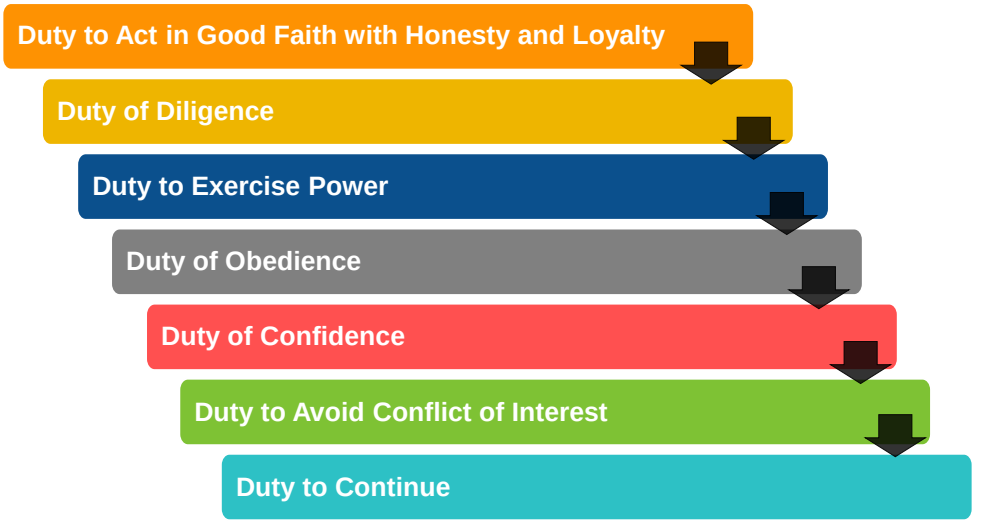
- Under the CNCA and the ONCA every director and officer of an NFP Corporation has a duty to "act honestly and in good faith with a view to the best interest of the corporation"
- This is the core duty that a director has under the CNCA and the ONCA and has its roots in the common law duty to act in good faith with honesty and loyalty, which will be discussed in a few minutes

**c) Statutory Standard of Care**

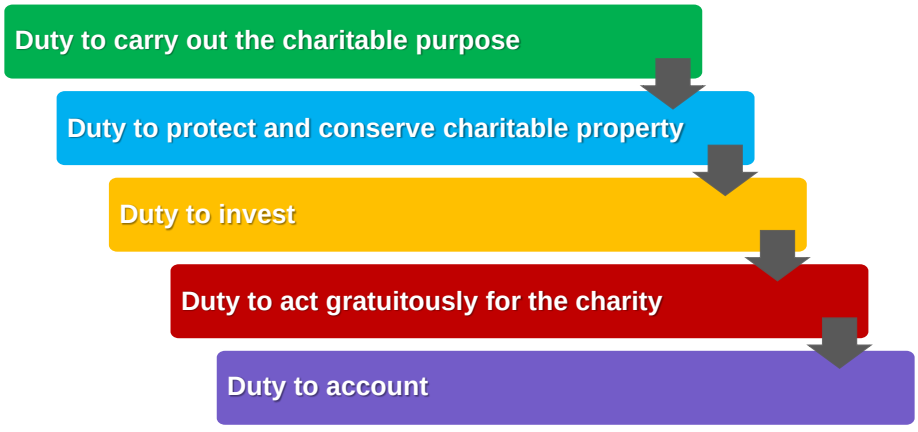
- Under the CNCA and the ONCA, every director and officer has a duty to exercise the "care, diligence and skill that a reasonably prudent person would exercise in comparable circumstances"
- Objective standard of care, same as business corporations



**3. Common Law Duties of Directors and Officers**



### 4. High Fiduciary Duties for Charities






## D. IT Governance Responsibilities

- Effective management of the NFP Corporation's IT infrastructure includes the following:
  - Approve, review and implement an IT governance policy/framework
    - Set out criteria and thresholds for IT decisions
    - How IT investment requests are initiated, review and approval process
    - Roles and accountabilities
    - Consider establishing an IT committee to lead IT decision making
  - Establish and approve the NFP Corporation's IT objectives
    - Identify corporate needs and demands
    - Select software and technology and ensure they align with business objectives
    - Be aware of technology trends e.g. AI

- Oversee IT resources and manage expenditures
  - Ensure adequate control of IT resources and that they are spent in accordance with the NFP Corporation's mission, purposes and objectives
  - Balance and prioritize resources and investments
  - Approve financial and investment decisions
  - Approve software, hardware and IT staffing requests
- Manage risk and compliance
  - Be informed about cybersecurity and other IT related risks and the NFP Corporation's exposure
  - Proactively identify, manage and mitigate IT related risks
  - Ensure that the NFP Corporation is compliant with laws and best practices
  - Put in place policies/procedures, including protocols for safeguarding personal information, protecting at-risk assets and responding to security breaches



## E. Practical Steps for Directors and Officers to Take in Managing the Risks

- In order to fulfill their fiduciary duties and avoid liability, directors of NFP Corporations must be able to demonstrate that they took appropriate steps to identify, manage and mitigate IT related risks
- The "Business Judgment Rule" – courts will not second guess boards that act prudently and on a reasonably informed basis
- Directors can show that they met the required standard of care and fiduciary duties by taking some practical steps:

a) Conduct an Audit

- First step is to develop a reasonable understanding of the NFP Corporation's assets and potential IT related risk exposures
- Understand how IT systems are utilized in the NFP Corporation's operations and the extent of its reliance on them

- Identify and categorize risks and their potential impacts, e.g.:
  - Risk of harms due to business interruption
  - Risk of harms due to failure to comply with legal, statutory or contractual obligations such as related to personal information, confidential business information
  - Categorize risk as “known-risks” and “unknown-risks”
- Audit systems and policies including cybersecurity, looking for potential weaknesses and failure points
- The board should understand what kind of data is held by the NFP Corporation, where it is held (e.g. cloud based vs. local servers), what jurisdiction is it in and how the data is protected
- Assess the robustness and resiliency of IT systems and infrastructure
- Audits can be conducted by internal IT staff or by external professional advisors
- The audit should evaluate the board’s level of competence and understanding of IT related topics and threats
- Post-audit, the board should analyze the report as well as recommendations made



b) Asset Management

- *Inventory and Track IT Assets*: Maintain an up-to-date inventory of hardware, software, and data assets to monitor usage, reduce redundancy, and ensure efficient resource allocation
- *Lifecycle Management:* Implement a clear process for the acquisition, maintenance, and disposal of IT assets. Regularly assess and upgrade systems to stay current and secure
- *Data Ownership and Accountability*: Define clear ownership and accountability for data assets. This establishes responsibility for security, accuracy, and compliance
- *Cost Control and Budgeting:* Proper asset management helps control costs by optimizing asset utilization and planning for future needs, ultimately contributing to financial sustainability
- *Compliance and Risk Management:* Managing assets effectively supports regulatory compliance (e.g., data protection laws to the extent that any are applicable) and minimizes risk exposure by ensuring regular security updates and timely decommissioning of outdated assets

c) Regular Education

- Boards have the obligation to develop an appropriate level of understanding of IT governance and risk issues
- Engage in ongoing education to enhance the board's understanding and competence related to IT governance
- Become informed about IT "best practices" and gain technological literacy
- Understand the relevant laws, regulations, government policies, accounting requirements, and other obligations that the directors and the NFP Corporation are required to comply with
- Training for employees and volunteers may also be needed as part of robust enterprise-wide privacy and cybersecurity policies



d) Establish an IT Governance Committee

- Include members with professional IT experience and expertise, as well as those with financial and legal knowledge
- Supported and authorized by the IT governance policy framework to make decisions, set standards and mitigate IT related risks
- Should include outside experts, senior management, as well as directors
- Report and make recommendations to the board

e) Reporting and Accountability

- Directors should obtain regular reports from management on IT related compliance and risk, including cybersecurity and privacy issues and reflect in board minutes
- Obtain confirmation from management that the NFP Corporation has appropriate privacy, IT security, cybersecurity preparedness, response and compliance measures in place
- Ensure that the NFP Corporation has in place a robust cybersecurity plan including investigating/responding to attacks and incidents
- Management should produce regular e.g. quarterly reports to the board on these issues, which should be reflected in board and committee minutes

f) Seek Expert Advice

- Obtain expert advice on IT risk management, including privacy and cybersecurity
- Obtain professional advice on insurance coverage, as noted below
- Carry out a robust review/audit of the NFP Corporation's IT infrastructure and policies
- Minutes should record that the expert met with the board, and advised the board on these issues

g) Insurance

- Confirm that the NFP Corporation has adequate cyber breach insurance in place to protect the NFP Corporation and the directors from IT related risks, such as a successful cyberattack on a business
- Seek professional advice from insurance brokers and insurers
- This is especially important for NFP Corporations that hold a significant amount of donor and/or client personal information or other sensitive data




## F. Key Takeaways

- Board Accountability: Boards must actively oversee IT Governance, ensuring policies are aligned with legal requirements and organizational goals
- Risk Management: Implement risk assessments and create proactive policies which limit and prevent risks from occurring
- Ensure Audits Occur: Audits of IT systems and Governance policies are essential to staying ahead of developing risks and requirements
- Continuous Education: IT Governance is a constantly evolving field, and boards must ensure they are up to date with new developments

Esther Shainblum, B.A., LL.B., LL.M., CRM – Ms. Shainblum is a partner at Carters Professional Corporation and practices in the areas of charity and not for profit law, privacy law and health law. She has been ranked by *Chambers and Partners.* Ms. Shainblum was General Counsel and Chief Privacy Officer for Victorian Order of Nurses for Canada, a national, not-for-profit, charitable home and community care organization. Before joining VON Canada, Ms. Shainblum was the Senior Policy Advisor to the Ontario Minister of Health. Earlier in her career, Ms. Shainblum practiced health law and corporate/commercial law at McMillan Binch and spent a number of years working in policy development at Queen's Park.

Contact information: eshainblum@carters.ca
1-877-942-0001

Cameron A. Axford, B.A., J.D. - Cameron is an associate whose practice focuses on Carter's knowledge management, research, and publications division. He articled with Carters from 2022 to 2023 and joined the firm as an associate following his call to the Ontario Bar in June 2023. Cameron graduated from the University of Western Ontario in 2022 with a Juris Doctor, where he was involved with Pro Bono Students Canada and participated in the BLG/Cavalluzzo Labour Law Moot. Prior to law school, Cameron studied journalism at the University of Toronto, receiving an Honours BA with High Distinction. He has worked for a major Canadian daily newspaper as a writer.

Contact information: caxford@carters.ca
1-877-942-0001



## Disclaimer

This handout is provided as an information service by Carters Professional Corporation. It is current only as of the date of the handout and does not reflect subsequent changes in the law. This handout is distributed with the understanding that it does not constitute legal advice or establish a solicitor/client relationship by way of any information contained herein. The contents are intended for general information purposes only and under no circumstances can be relied upon for legal decision-making. Readers are advised to consult with a qualified lawyer and obtain a written opinion concerning the specifics of their particular situation.