# Canadian Tire Corporation

## Company Type and Stakeholders

## Prepared for Senior Management and Executives

# Table of Content

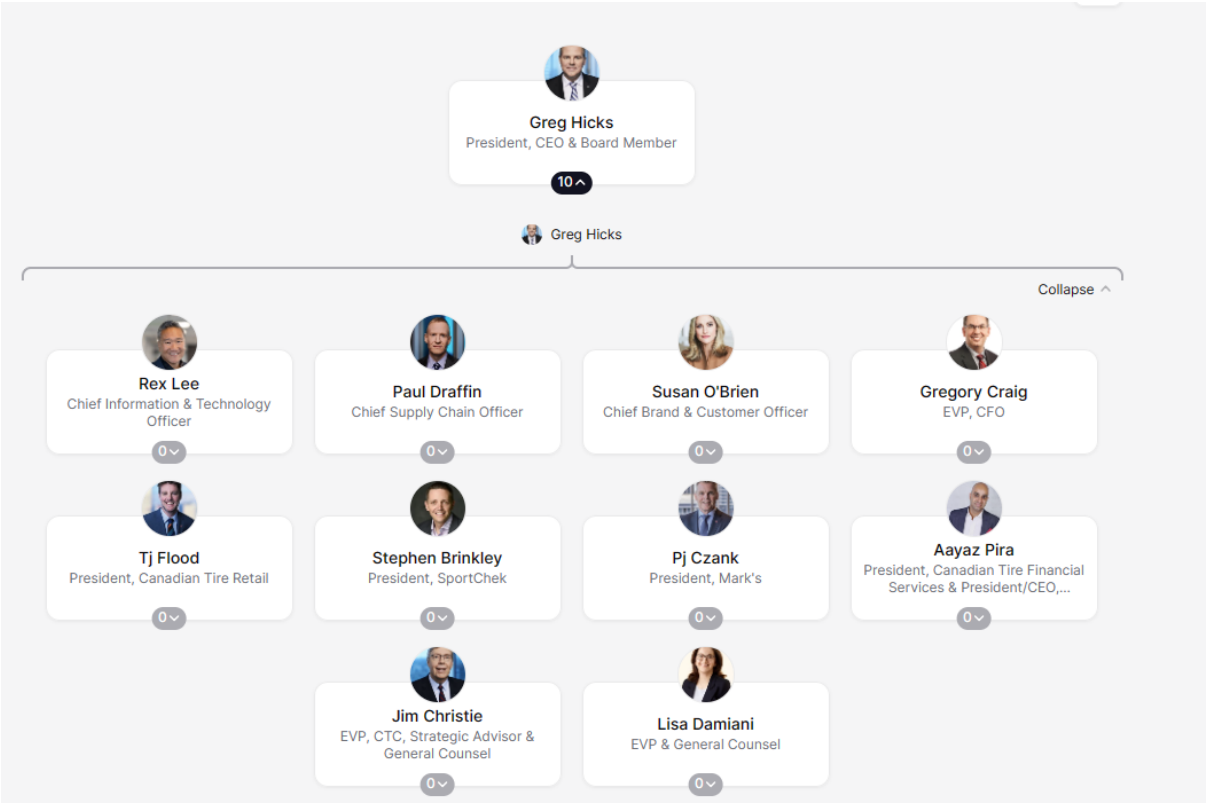
# Executive Summary:

In the dynamic and ever-evolving landscape of modern business, the need to safeguard our organization against a spectrum of security incidents is paramount. As the Canadian Tire Corporation, a prominent and diversified Canadian conglomerate, operates across multiple sectors, the complexities and vulnerabilities associated with our business activities necessitate a comprehensive approach to security incident preparedness and response. This report explores how various elements, including our size, structure, industry presence, stakeholders, ownership model, legal and regulatory compliance, potential incidents, and their relative impacts, and the distinction between internal and external incidents, and industry-specific occurrences, interplay in forming a robust security incident strategy. By understanding and addressing these factors, we can strengthen our resilience and safeguard our reputation.

# 1. Company Size, Structure, Industry, and Area of Business:

Canadian Tire Corporation's expansive reach spans multiple sectors, including automotive, retail, and financial services, with about $13.7B in revenue, $16.3B in assets, and $802M in profit as at October 2023. Our organizational structure comprises numerous subsidiaries and divisions, including Canadian Tire Retail, Mark's, FGL Sports, and Canadian Tire Financial Services account fo about 34,606 employees. This diversified model exposes us to a broad range of potential security incidents, each unique to the sector in which it occurs.

Org Chart




# 2. Company Stakeholders and Ownership Model:

As a publicly traded entity, we engage a complex web of stakeholders, encompassing shareholders, customers, employees, and regulatory authorities. Our ownership structure demands a high level of transparency, compelling us to promptly report incidents and breaches. This transparency not only satisfies legal obligations but also underscores our commitment to integrity, reinforcing trust among shareholders and customers.

Stakeholder:

1. Shareholders: As owners of the company's publicly traded shares, they have a vested interest in the organization's performance and reputation.
2. Customers: The lifeblood of the retail and financial services divisions, their trust and satisfaction are paramount.

3. Employees: The organization's workforce, from store staff to executives, plays a crucial role in ensuring smooth operations and customer interactions.
4. Regulatory Authorities: Bodies such as the Office of the Privacy Commissioner of Canada (OPC) oversee compliance with data protection regulations and reporting standards.
5. Chief Information Officer (CIO): Responsible for the management and protection of the company's data and information systems.
6. Supply Chain Partners: Critical stakeholders for an organization reliant on a smooth and efficient supply chain.
7. Industry-Specific Watchdogs: Organizations such as the Canadian Motor Vehicle Arbitration Plan (CAMVAP) monitor industry-specific incidents and disputes.

Canadian Tire, being a publicly traded company, has a responsibility to uphold transparency and adhere to regulatory reporting standards. Consequently, the selection of stakeholders, including shareholders and regulatory authorities, is influenced as they anticipate timely and thorough incident reporting.

# 3. Laws and Regulations:

Operating within an industry governed by a multitude of laws and regulations, Canadian Tire Corporation must rigorously adhere to consumer protection laws, privacy regulations, and financial industry standards. Strict compliance with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) is imperative, particularly in privacy breach incidents. A deep understanding of these regulations is pivotal in shaping our incident response strategy.

# 4. Potential Incidents and Their Relative Impacts:

Our organization faces a diverse range of potential security incidents. Data breaches could compromise customer data within the financial services division, resulting in severe reputational damage and regulatory penalties. Cyberattacks

may disrupt e-commerce operations, leading to financial losses and eroding customer trust. Supply chain disruptions can impede product availability in Canadian Tire Retail stores, bearing both operational and financial ramifications. In-store security incidents might compromise the safety of employees and customers, potentially causing lasting harm to our brand's reputation.

Specific Incident Types:

1. Data Breach:
Immediate Notification: Chief Information Officer (CIO), Regulatory Authorities, Shareholders
Post-Incident Notification: Customers, Employees

2. Cyberattack:
Immediate Notification: CIO, Regulatory Authorities, Shareholders
Post-Incident Notification: Customers, Employees

3. Supply Chain Disruption:
Immediate Notification: Supply Chain Partners, Regulatory Authorities
Post-Incident Notification: Customers, Employees

# 5. Internal vs. External Incidents and Industry-Specific Occurrences:

We must discern between internal and external incidents and industry-specific events. Internal incidents, such as employee misconduct, have the potential to undermine organizational integrity and affect employee morale. External incidents, including cyberattacks and supply chain disruptions, possess the capability to disrupt entire business operations. Industry-specific incidents, such as recalls of automotive parts or safety concerns with products sold in Canadian Tire Retail stores, bring about sector-specific regulatory and reputational consequences.

# Recommendations:

In light of the complex and multifaceted security landscape we operate within, we recommend the following actions to enhance our security incident preparedness and response:

1. Comprehensive Incident Response Plan: Develop and maintain a robust and comprehensive incident response plan that accounts for the diverse nature of our business operations and includes specific protocols for addressing incidents unique to each sector.

2. Stakeholder Engagement: Proactively engage all stakeholders, including shareholders, customers, employees, and regulatory bodies, in the incident response process to ensure transparency and trust-building.

For each specific incident type, recommendations are as follows:

Data Breach:

- Notify CIO, Regulatory Authorities, and Shareholders immediately.
- Inform affected Customers and Employees post-incident, providing guidance and support.

Cyberattack:

- Notify CIO, Regulatory Authorities, and Shareholders immediately, along with detailed information.
- Communicate with Customers and Employees post-incident, outlining protective measures.

Supply Chain Disruption:

- Notify Supply Chain Partners immediately, collaborating on mitigation efforts.
- Inform Regulatory Authorities of the incident for compliance purposes.

Maintaining a transparent and proactive communication strategy with all stakeholders is essential in every situation. This approach not only minimizes the impact of security incidents but also enhances Canadian Tire's reputation as a trustworthy and accountable corporate entity.

3. Ongoing Compliance Education: Invest in ongoing education and training programs to ensure our teams are well-versed in industry-specific regulations, reporting standards, and best practices for incident management.

4. Regular Drills and Simulations: Conduct regular incident response drills and simulations across all divisions to test the effectiveness of our response protocols and identify areas for improvement.

5. Communication Strategy: Develop a strategic communication plan that addresses both internal and external stakeholders during and after security incidents, ensuring timely and accurate dissemination of information.

# Conclusion:

A proactive and comprehensive approach to security incident management is not just a matter of compliance but a fundamental element of safeguarding our reputation, customer trust, and business operations. By understanding and addressing the factors outlined in this report, we can enhance our security incident preparedness and response and further solidify our standing as a trustworthy and responsible corporate entity.

Prepared by: Victor Onukwu

Date: October 23, 2023