Nearly 1 in 3 focused breach attempts succeed. Yet, most Canadian companies are confident in their ability to protect the enterprise. Yet, only 22% would invest in mitigating financial loss, and nearly 1 in 3 focused breach attempts succeed. In a cybersecurity survey, Canadian respondents express con
difidence in their abilities to protect the enterprise. 96% of respondents said that a breach is a threat to their organization.

**Reboot Your Approach: Deal Effectively With Threats**

1. **Define Cybersecurity Success**
   - Establish clear objectives and performance targets.
   - Align with business goals and stakeholders.

2. **Pressure-Test Security Capabilities**
   - Conduct regular assessments and simulations.
   - Evaluate effectiveness against realistic scenarios.

3. **Protect from the Inside Out**
   - Identify and mitigate internal vulnerabilities.
   - Ensure that access controls are robust and monitored.

4. **Build Ownership**
   - Empower all employees to take a proactive role in security.
   - Foster a culture of security awareness and accountability.

5. **Make Security Everyone’s Responsibility**
   - Engage “white-hat” hackers for external assessments.
   - Implement comprehensive detection and prevention policies.

6. **Leverage Your Cyber-Competitors**
   - Learn from industry peers and benchmark practices.
   - Collaborate with partners to share insights and develop strategies.

**Invest to Innovate and Outmaneuver**

1. **Define the Risk Landscape**
   - Conduct an organizational assessment of risk.
   - Prioritize efforts based on potential impact.

2. **Develop a Cybersecurity Roadmap**
   - Align investments with business objectives.
   - Define measurable milestones and targets.

3. **Ensure Compliance and Legal Readiness**
   - Understand regulatory requirements and contractual obligations.
   - Implement policies to mitigate legal and reputational risks.

4. **Steer a Course for Innovation**
   - Prioritize development of novel solutions.
   - Invest in research and development.

5. **Build a Cybersecurity Culture**
   - Foster a culture of security awareness and accountability.
   - Implement training programs to enhance employee capabilities.

**Build Confidence in the Security Organization**

1. **Establish a Security Governance Program**
   - Define roles, responsibilities, and accountability structures.
   - Establish clear lines of authority and decision-making processes.

2. **Engage the C-suite and Board**
   - Keep the board informed and aligned with business strategy.
   - Ensure that the C-suite supports ongoing cybersecurity initiatives.

3. **Communicate Effectively**
   - Develop a coordinated communication strategy.
   - Ensure that messaging is clear and consistent across all stakeholders.

4. **Develop a Resilience Strategy**
   - Identify critical business processes and assets.
   - Implement measures to minimize downtime and financial impact.

5. **Prepare for Incidents**
   - Create a robust incident response plan.
   - Practice scenarios to effectively manage cyber-attacks.

**Conclusions**

- Most companies believe they can protect key assets, but only 40% have developed a clear plan to protect and recover key assets.
- Only 29% have a clear business-relevant threat monitoring program in place.
- Cybersecurity strategies and investments are often siloed, with limited integration across the organization.
- There is a misalignment between the cost of a targeted attack and the ability to mitigate financial loss.
- Canadian respondents expressed high levels of confidence in their ability to protect the enterprise, yet only 22% would invest in mitigating financial loss.

**Implications**

- There is a need for a more holistic approach to cybersecurity, incorporating both technical and non-technical solutions.
- Companies should prioritize investments in personnel training and culture change to improve overall maturity.
- Leadership and management must be actively engaged in the development and implementation of cybersecurity strategies, ensuring alignment with business objectives.
- A more comprehensive approach to compliance frameworks and agreements is needed to address the rapidly evolving legal landscape.

**Recommendations**

- Companies should adopt a proactive stance towards cybersecurity, focusing on prevention, detection, and response.
- Investments in technology and personnel training should be aligned with business imperatives.
- Cybersecurity governance should be embedded into the culture and decision-making processes of organizations.
- Leadership should prioritize cybersecurity as a critical business priority, with CISOs as strategic business partners.

**Conclusion**

By adopting a comprehensive and aligned approach to cybersecurity, organizations can better protect their assets and improve overall business performance.