




Managing cyber risk  
in Canada's new  
cannabis sector

**EY**

Building a better  
working world





Recent cyber events have highlighted the impact on business operations, process automation, data protection and privacy. These incidents are not limited to a single sector, geography, size or scale. So it's necessary to go back and review the basics around issues such as governance and hygiene. Cyber attacks are becoming more prevalent, severe, and sophisticated.

Cyber events are hitting companies' bottom line, brand and reputation and are reverberating across our ecosystem. All executives should be concerned.

EY's *Global Information Security Survey*<sup>1</sup> revealed how Canadian executives are dealing with cyber risks today. Some of the findings were surprising:

- ▶ 16% of respondents believe their boards have sufficient information security knowledge to fully evaluate cyber risks
- ▶ 89% of respondents say they need additional funding to protect their organization

Some of the key characteristics of the cannabis sector and its operations are companies' access to a large amount of intellectual property, research, personal and patient data, and financially sensitive information – all of which make them especially attractive targets for cyberattacks. Breaches can disrupt business operations, hackers can threaten to release sensitive data, steal data, cause system outages or block access to data until a ransom is paid. Cyber incidents like these diminish trust and reputation for any company; for those that are representing a new market, the risk is even greater.

So the question is, what areas should cannabis companies focus on to effectively manage cyber risk?

Whether your organization develops cybersecurity management capabilities in house or relies on a third-party managed service, we've identified the top five key success factors for a cyber-resilient cannabis organization.

<sup>1</sup> EY's 21st Global Information Security Survey captures the responses of nearly 1,400 C-suite leaders and Information Security and IT executives/managers, representing most of the world's largest and most recognized global organizations.

# 01

## Robust governance framework



Good governance starts with the tone at the top. Awareness and understanding of cybersecurity risk, strategy and operations at the board level is essential to the overall functioning of a cyber-resilient company.

For cannabis companies, this awareness and understanding should be more pronounced, given the medical, customer, personal, financial, transactional and proprietary data involved in daily operations. This plethora of sensitive information makes cannabis companies a tempting target for cyberattacks.

Cybersecurity awareness and education of executives and board directors of cannabis organizations will help to establish a cybersecurity program that is intertwined with the organization's operations and not considered as an afterthought.

Companies need to recruit and develop talent that understands the importance of cybersecurity and perpetuates a proactive, risk-aware culture. Boards, executives and risk committees want a clear picture of the cyber-risk exposure and how the company's cyber program addresses these risks.

# 02

## Strategic intellectual property protection



Cannabis will be exposed to supply-demand price pressures. Intellectual property and research and development will be sources of long-term competitive advantage in this high-growth industry. Since the majority of companies are racing to develop cannabis-derived products that qualify for patents or drug identification numbers – the latter will make the product exempt from excise taxation and more likely to be covered by medical insurers – and export knowledge (e.g., standard operating procedures), they should be aware of their cyber risks.

Recognizing the strategic benefits of investment in information security is of paramount importance. Including information security in the planning of overall strategy will aid cannabis companies in realizing savings from thwarted security incidents and resulting financial damage.

Due diligence and setting your organization up with the necessary tools to prevent, monitor, detect and resolve breaches or incidents requires annual planning and spend. Building a prioritized roadmap for investments in cybersecurity requires strategic budgeting for information security operations in line with the requirements of the organization and fosters organizational change.

# 03

## Risk-focused innovation



Some of the early cultivation facilities were existing manufacturing facilities or greenhouses that were retro-fitted for cannabis cultivation. Advancements in technology have prompted licensed producers to upgrade their facilities with more innovative technologies. Newly licensed cultivation facilities are built with state of the art equipment, machinery and environmental systems, which enable a higher level of automation and advanced crop monitoring.

Utilities, wages and salaries are currently two of the biggest cost drivers of operational expenses for operators in the cultivation segment of the cannabis value chain. Applications of innovative technologies such as Internet of Things (IoT), blockchain, robotic process automation (RPA), artificial intelligence (AI) and machine learning offer many advantages in terms of cost-cutting and efficiency with respect to automating manual and labour-intensive activities.

Cultivation with a degree of automation can include various smart technologies, including utility consumption management, connected HVAC, lighting, drip irrigation and nutrient systems, and environmental controls over humidity and temperature. All of these areas are at risk of being hacked. Cannabis is a very difficult plant to optimize, and due to pharma-like regulations in an agricultural environment, disruptions can ruin entire crops or grow rooms and result in unsellable products.

Any implementation of technology carries inherent security risks. Cannabis companies should be cognizant of aligning their cybersecurity strategy with their business objectives as they incorporate more automation and connected technologies in their cultivation, processing, testing, supply chain and retail operations. Having in-depth experience in the strategic planning of security measures and risk mitigation will help cannabis companies efficiently use these technologies while putting the right systems and tools in place to protect their business.

# 04

## Risk identification and management



Cannabis companies that engage external partners, vendors or contractors who can support their growth and rapid scaling should be cognizant of managing third-party risk. They can tap into the benefits of enterprise resource planning systems for integrated business processes, servers to host patient and customer data, vendor management programs to automate operational finance and procurement functions, and other various third-party services.

Cannabis companies must have a good understanding of the responsibilities and boundaries of their own cybersecurity environment and have insight into the control environments of their service organizations. There should also be a focus on maintaining an accurate inventory of third-party service providers, network connections and data.

Intelligence-driven cybersecurity functions are equipped with systems and tools that enable real-time monitoring of network connections and data, and rapid threat identification, response and resolution.

Internal cybersecurity enablers and programs include:

- ▶ Threat and vulnerability management for malicious attacks
- ▶ Identity and access management to monitor your facility's perimeter and rooms throughout the vegetation-flowering-drying/curing lifecycle and comply with Health Canada's security requirements
- ▶ Advanced predictive analytics and artificial intelligence in combination can identify threat patterns and attacker techniques while crawling the deep/dark web and accelerate the discovery of imminent attacks

Guarding against all sources of information security risks, both internal and external, will elevate the cybersecurity resilience of cannabis organizations.

# 05

## Resiliency and business continuity



Customers' personal identifiable data is of high value to cyber criminals. Ransomware attacks such as WannaCry exposed the vulnerabilities of organizations that were running outdated technology and had aging infrastructure, crippling their day-to-day operations. This incident triggered a massive effort to reorganize and update cybersecurity measures.

Cannabis companies can become more strategic in their response to cybersecurity incidents by being less reactionary. This can be to their benefit as they proactively defend against their greatest risks and make them focus areas for building resilience.





# How EY can help

Our Cybersecurity Transformation professionals are focused on bringing our clients' cybersecurity to the next level. We bring deep experience across a wide range of services, including the following:

- ▶ **Developing** a clear focus on protecting business goals and objectives, not just corporate data centers.
- ▶ **Implementing** innovations such as RPA, IoT, AI and blockchain technologies to detect and respond to cyber incidents and threats.
- ▶ **Optimizing** protection by allocating capital where it makes most sense.
- ▶ **Creating** an integrated cybersecurity strategy that underpins your growth ambitions by making new digital channels/connections secure, supporting new business models with innovative cybersecurity or supporting the wish to be agile.
- ▶ **Gaining visibility** into your current-state posture and board-endorsed increased investment in advancing capabilities.
- ▶ **Aligning** multi-year programs to focus on protection, optimization and growth.
- ▶ **End-to-end cyber services** across consulting, implementation and managed services.

A photograph of two men in dark blue suits standing in a factory or industrial setting. They are looking at a tablet held by the man on the right. The background shows industrial equipment, pipes, and a blue and white striped ceiling. The text is overlaid on the left side of the image.

# Ingredients required to manage cyber risk and achieve cybersecurity resilience

Organization's objectives

Secure engagement with customers

Robust growth agenda

Regulatory compliance

Supporting innovation

Increased brand protection and trust

5

### Resilient and scalable

Helps minimize the impact of disruptions and keeps pace with business growth

- Incident response
- Cyber crisis management
- Resiliency and continuity
- Capital and liquidity management
- Recovery and resolution

2

### Strategic and innovative

Embedded in strategic decision-making and benefits from and adopts ongoing innovation

- Linked to strategy
- Cybersecurity due diligence
- Digital transformation
- Robotic process automation (RPA)
- Smart devices, operational technology, blockchain and distributed ledger
- New product development
- Innovation and ideation

1

### Talent centric

Built on a foundation that makes cybersecurity everyone's responsibility

- Talent management
- Board and 3LoD\* roles and responsibilities
- Risk and security culture
- Training and awareness

4

### Intelligent and agile

Situationally aware and intelligence driven cybersecurity function that enables timely threat identification and response

- Cyber threat intelligence
- Threat and vulnerability management
- Identity and access management
- Security operations and managed services
- Technology architecture

3

### Risk focused

Driven by well-governed risk alignment, risk awareness and risk prioritization

- Governance
- Cyber-risk management and appetite
- Policies and standards
- Metrics and reporting
- Third-party risk management
- Regulatory awareness

Organization's outcomes

Increased shareholder value

Improved regulatory alignment

Effective risk management

Enhanced branding

\*Three lines of defense

**About EY**

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.

For more information about our organization, please visit [ey.com/ca](http://ey.com/ca).

© 2018 Ernst & Young LLP. All Rights Reserved.  
A member firm of Ernst & Young Global Limited.

2898844  
ED None

This publication contains information in summary form, current as of the date of publication, and is intended for general guidance only. It should not be regarded as comprehensive or a substitute for professional advice. Before taking any particular course of action, contact EY or another professional advisor to discuss these matters in the context of your particular circumstances. We accept no responsibility for any loss or damage occasioned by your reliance on information contained in this publication.

[ey.com/ca](http://ey.com/ca)

**Learn more**

For more information, please contact a member of our team:



**Monica Chadha**  
National Cannabis Leader  
+1 416 943 3496  
[monica.chadha@ca.ey.com](mailto:monica.chadha@ca.ey.com)



**Bryson Tan**  
+1 416 943 3925  
[bryson.tan@ca.ey.com](mailto:bryson.tan@ca.ey.com)



**Helen Goloubtchik**  
+1 416 943 2077  
[helen.goloubtchik@ca.ey.com](mailto:helen.goloubtchik@ca.ey.com)



**Ashley Chiu**  
+1 416 943 5307  
[ashley.chiu@ca.ey.com](mailto:ashley.chiu@ca.ey.com)

