CANNABIS NEWS YOU CAN USE
CANNABIS
RISK MANAGER

Protecting Your Cannabis Company: 7 Cybersecurity Steps

Protecting Your Cannabis Company: 7 Cybersecurity Steps to Safeguard Your Business and Data

As the cannabis industry grows, so do the cyber risks facing operators, dispensaries, cultivators, and support businesses. With valuable data—from patient records to proprietary cultivation processes—your company is an attractive target for cybercriminals. A single breach can disrupt operations, damage your reputation, and result in regulatory fines. Fortunately, implementing proactive cybersecurity practices can drastically reduce your exposure. Here are seven key steps cannabis companies should take to protect themselves.

1. Revisit Your Incident Response Plan to Ensure Rapid and Effective Action During Cyber Events

Even the most secure cannabis companies can face cyber incidents. Whether it’s a ransomware attack, phishing breach, or system failure, having a robust incident response plan (IRP) ensures your team knows exactly what to do.

- Confirm that your IRP is up-to-date, listing roles, escalation paths, contacts, and communication channels.
- Test monitoring and escalation procedures, including coverage during holidays or off-hours.
- If you use third-party vendors or managed IT services, verify how they handle after-hours alerts and who is on call when your office is closed.

A prepared response can be the difference between a minor disruption and a full-blown operational crisis.

2. Audit User Access and Permissions to Strengthen Digital Doors Across Your Network

Cybersecurity begins with controlling who can access your systems. Regularly auditing user accounts ensures that only authorized personnel have access to sensitive data and systems.

- Remove accounts for employees or contractors who have left the company.
- Review administrative privileges and confirm that users still need elevated access.
- Enforce multi-factor authentication (MFA) across all accounts, especially for remote employees.

Research from Microsoft shows that 99.9% of compromised accounts lacked MFA. This single, simple safeguard is one of the most effective ways to prevent breaches.

3. Prepare Your People to Recognize and Avoid Phishing Attacks and Other Social Engineering Threats

Employees are often the first line of defense—or the weakest link—in cybersecurity. Phishing scams frequently spike during the holiday season, using fake promotions, shipping updates, or HR messages to trick users.

- Send refresher training on spotting suspicious links, attachments, or emails.
- Encourage verification of requests for gift cards, donations, or sensitive information.
- Remind staff to report suspicious activity rather than just deleting it.

Consider structured security awareness programs to keep employees vigilant year-round, creating a culture of cybersecurity mindfulness.

4. Test Backups and Recovery Systems to Mitigate the Impact of Ransomware and Other Data Loss Events

Ransomware attacks remain one of the costliest cyber threats to cannabis businesses. Having reliable backups and recovery processes is essential to minimize downtime.

- Verify that all backups are running properly and include critical cloud and on-premise data.
- Store at least one backup offline or in a securely segmented environment.
- Conduct a five-minute restore test to ensure that you can recover quickly.

Regular testing ensures that your company can restore operations quickly, protecting both your revenue and your patients' access to products.

5. Secure Remote and Mobile Access to Protect Your Network Perimeter Beyond the Office

Cannabis employees often work remotely, from home offices, coffee shops, or while traveling. Each endpoint outside your corporate network represents a potential vulnerability.

- Require VPN connections and strong device encryption for all remote access.
- Patch and update all devices, including personal devices with company access.
- Consider implementing endpoint detection and response (EDR) tools for continuous threat monitoring.

According to Verizon's Data Breach Investigations Report, over 80% of breaches involve compromised credentials or unpatched software. Maintaining strict remote access policies is a simple, effective defense.

6. Monitor Your Systems Around the Clock to Detect and Respond to Threats in Real Time

Cyber threats never sleep. Continuous monitoring ensures that suspicious activity is detected early and mitigated before damage occurs.

- Set up 24/7 alerts for anomalies, failed login attempts, and new device connections.

- Automate threat detection, patch management, and log analysis to reduce response time.
- If internal resources are limited, partner with a managed detection and response (MDR) provider for continuous coverage.

Whether monitored in-house or through a third-party service, constant vigilance allows you to respond quickly, minimizing the impact of potential breaches.

7. Plan for the New Year to Strengthen Cybersecurity Posture and Budget for Emerging Threats

The quieter periods after holidays provide an ideal opportunity to evaluate lessons learned and plan for the next year.

- Conduct a post-holiday audit to review any incidents, gaps, or near misses.
- Allocate budget for upgrades, training, and assessments to stay ahead of evolving threats.
- Refresh policies, user education, and emergency protocols to start the new year with a stronger security posture.

Using these insights to inform your 2026 cybersecurity strategy ensures your cannabis company remains resilient against emerging threats.

Cybersecurity as a Continuous Commitment for Cannabis Operators

The cannabis industry faces unique risks, from protecting patient data to safeguarding proprietary cultivation processes. By following these seven cybersecurity steps—revisiting your incident response plan, auditing user access, preparing your people, testing backups, securing remote access, monitoring systems continuously, and planning for the new year—cannabis companies can significantly reduce their exposure to cyber threats.

Implementing these practices requires ongoing attention, collaboration with IT experts, and commitment from leadership. Companies that make cybersecurity a priority will protect their operations, their reputation, and their customers, ensuring they can thrive in the rapidly evolving cannabis marketplace.

For practical tools, checklists, and professional guidance, cannabis operators can reach out to trusted cybersecurity advisors or visit resources like Cannabis Risk Manager to get started.