CANNABIS NEWS YOU CAN USE
CANNABIS RISK MANAGER

Digitizing Cannabis Businesses Without Opening Doors to Hackers

Cannabis Industry's Digital Shift Brings New Efficiencies and New Cyber Threats

Along with new efficiencies and growth opportunities, the cannabis industry's rapid digital transformation is creating a formidable new challenge for operators: cybersecurity.

Retailers' increasing reliance on integrated digital platforms for critical functions—such as point-of-sale (POS) transactions, digital payments and customer loyalty programs—is turning them into prime targets for sophisticated cybercriminals.

With vast amounts of customer data at stake, the potential for costly and damaging data breaches has never been higher, operators and security experts warn.

"Retail in general continues to be a very big target for cybercriminals," said Ben Taylor, executive director of the Virginia-based Cannabis Information Sharing & Analysis Organization (Cannabis ISAO), a nonprofit that supports the industry's security efforts.

Digital Transformation Unlocks Efficiency, but Expands Exposure

The cannabis industry has long operated in a largely cash-based, brick-and-mortar environment. But the modern dispensary is now a complex digital ecosystem.

E-commerce platforms, online ordering systems, integrated payment tools and data-driven marketing technologies have become mainstream—unlocking new levels of operational efficiency and customer engagement.

However, each digital interaction creates data: purchase histories, personal identification details, contact information and other sensitive customer insights. For cybercriminals, this is a valuable trove.

Several recent incidents underscore the risks.

Earlier this year, Los Angeles based operator Stiiizy notified the Maine Attorney General of a data breach affecting roughly 380,000 users after an attack on a POS software vendor. While details remain limited, observers believe ransomware may have been involved.

In a separate case, an Ohio-based medical cannabis recommendation company reportedly left nearly 1 million sensitive records in a publicly accessible database—triggering a state investigation and multiple lawsuits.

Beyond financial and reputational consequences, breaches in cannabis carry another layer of risk: the exposure of customer information linked to a federally illegal substance. Such incidents can result in serious privacy violations, legal liabilities and long-term damage to consumer trust.

Tech Providers Turn to New Cyber Defense Strategies

Recognizing the escalating threats, some cannabis technology companies are taking a more proactive approach.

Sweed, a retail technology platform, recently launched a public “bug bounty” program. The initiative invites ethical hackers and security researchers from around the world to probe Sweed’s web services and data infrastructure for vulnerabilities. Rewards of up to $2,000 are paid based on the severity of the issues discovered.

The goal, according to Sweed co-founder Rocco Del Priore, is twofold: improve software resilience and strengthen customer trust.

“As the industry matures, it’s becoming more corporate, involves more public companies and relies more heavily on processes,” Del Priore said. “We’re mature enough and confident enough in our platform that we’re inviting anyone anywhere in the world to come break it.”

Taylor of Cannabis ISAO said bug bounty programs like Sweed’s enhance transparency and demonstrate a commitment to data protection.

“Speed to market is so important for these software companies,” he noted. “That bottom line is really pushing things, and security can fall by the wayside.”

Why Retailers Must Take a More Active Role in Cyber Defense

Cybersecurity experts stress that dispensaries and multistate operators (MSOs) also play a crucial role in protecting sensitive data.

“You can have the most robust compliance in the world, but if your network is vulnerable or your POS can be breached, your entire business and customer trust are on the line,” Taylor said.

The growth of e-commerce and digital ordering has attracted more advanced threat actors. A single exploit can expose not only financial data but also medical information, customer identities and internal business operations.

Eric LaForce, head of engineering at cannabis wholesale platform LeafLink, said cybersecurity will only grow in importance as the industry ages and consolidates.

One persistent challenge for MSOs is navigating the patchwork of state regulations governing cybersecurity. LaForce said companies can reduce risk by developing internal cybersecurity standards that apply across all operating states.

“It makes it easier to know what you’re supposed to do,” he said.

Practical Steps Cannabis Retailers Can Take Now

Security experts say there are several foundational steps cannabis operators should prioritize:

1. Invest in Employee Training

Staff remain the first line of defense. Training employees to spot phishing scams, use strong passwords, manage access privileges and understand privacy protocols can prevent many common breaches.

2. Choose Technology Partners Carefully

Retailers should thoroughly vet POS, e-commerce and marketing vendors. Key questions include:

- Do they conduct regular penetration tests?
- Do they have a dedicated security team?
- How quickly do they patch vulnerabilities?

3. Create and Maintain an Incident Response Plan

No system is fully breach-proof. Retailers should have a clear plan for:

- isolating compromised systems
- notifying customers and regulators
- restoring operations quickly
- documenting the incident

Too many operators, LaForce said, do not think about cybersecurity until after an incident.

For more information contact at info@cannabisriskmanager.com

Email: info@cannabisriskmanager.com | Phone: +415-226-4060