GROWERTALKS

Features

6/30/2025

Protecting Your Business From Threats

Dan Zastava

In today's digital landscape, cybersecurity is no longer a concern exclusive to large corporations. No matter the size of your horticulture business, if you store any data online—such as customer personal information, credit card details or vendor payment methods—you're at risk of a cyberattack. As cybercriminals increasingly target small and mid-sized businesses due to their often weaker security measures, cybersecurity for greenhouse growers has never been more critical.

In fact, a majority of small business owners (60%) say cybersecurity threats are a top concern. By definition, horticulture businesses fit this demographic: small and local, often lacking the robust cybersecurity defenses of larger corporations. Understanding the common cybersecurity threats and implementing proactive measures is essential to safeguarding your business, employees and customers.

Common cybersecurity threats

Cybercriminals exploit weaknesses in digital systems—especially outdated software—to access sensitive information. They employ a variety of attack methods, with the following being the most common:

- **Phishing scams:** Phishing scams involve fraudulent emails or messages designed to trick employees into revealing sensitive data, such as login credentials or payment details. These messages often appear to be from trusted sources, such as suppliers or financial institutions, and contain urgent requests for action. Clicking on malicious links or downloading infected attachments can compromise your entire business network.
- **Fraudulent impersonation:** Cybercriminals often impersonate business executives, vendors or even customers in an attempt to extract money or sensitive information. A common tactic is sending fake invoices that appear legitimate, prompting employees to process fraudulent payments. In the horticulture industry, where multiple vendors and suppliers are involved, using two-factor authentication to verify financial transactions is a great way to avoid falling victim to such schemes.
- **Ransomware attacks:** Ransomware is a type of malicious software (malware) that encrypts a company's data, making it inaccessible until a ransom is paid. Hackers may threaten to delete, expose or permanently encrypt essential files, paralyzing business operations. For greenhouse operators, garden centers and nurseries, the inability to access customer data, inventory records or vendor transactions can cause significant disruption and financial loss.

- **Man-in-the-middle attacks:** This type of attack occurs when a cybercriminal intercepts sensitive information during transmission. Unsecured websites and public WiFi networks can be exploited to gain access to financial transactions, customer data or order details. If your business relies on an online ordering system, securing your network connections is vital.

How to reduce the risk of a cyberattack

Cybersecurity is a collective effort, requiring awareness and vigilance from every member of your team. Here are six essential strategies to mitigate greenhouse cyber threats:

1. Educate and train employees

- Conduct regular cybersecurity training to help employees recognize phishing attempts and suspicious activity.
- Establish clear policies on data security, acceptable use and safe browsing practices.
- Encourage employees to report suspicious emails, messages or phone calls immediately.

2. Keep software and systems updated

- Boost technology security by keeping operating systems, anti-virus software and applications updated regularly.
- Install security patches promptly to close vulnerabilities that hackers could exploit.
- Implement automatic updates to reduce the risk of outdated software being targeted.

3. Perform regular data backups

- Schedule automated backups of critical data to secure, off-site storage locations.
- Maintain multiple backup copies, including one isolated from the cloud or internet.
- Periodically test data restoration processes to ensure they function correctly in an emergency.

4. Secure data storage and access

- Assess whether you need to collect and store sensitive customer data. If not, avoid gathering unnecessary information.
- Implement encryption and multi-factor authentication (MFA) to protect stored data from unauthorized access.
- Regularly update security settings and user permissions to limit exposure.

5. Strengthen password policies

- Encourage employees to create strong, unique passwords and update them regularly.
- Use passphrases with a combination of random words, numbers and symbols.
- Deploy password managers to store and generate complex passwords securely.

6. Verify communications and transactions

- Scrutinize all email requests for urgent financial transactions or sensitive data.
- Contact vendors or clients directly using trusted contact information to verify requests.
- Implement a two-step verification process for significant financial transactions.

Cyber insurance: An added layer of protection

Cyber liability insurance is an essential component of a robust cybersecurity strategy. Just as traditional greenhouse business insurance protects against physical damage, cyber insurance helps cover financial losses resulting from cyber incidents.

Cyber insurance for agriculture businesses may cover:

- Business interruption: Helps compensate for lost revenue during downtime caused by cyberattacks.
- Regulatory fines: Provides assistance in paying fines resulting from data breaches.
- Customer notifications: Covers the costs of informing customers of breaches and offering credit monitoring.
- Data recovery: Pays for specialists to recover or restore lost or encrypted data.
- Ransomware payments: May help reimburse businesses forced to pay ransom demands.

Before purchasing cyber insurance, review policy details carefully to understand coverage limits and exclusions. Additionally, some insurance providers offer cybersecurity training and preventive resources to help businesses reduce the likelihood of an attack, so it's important to know how to talk to your insurance provider.

Developing a cybersecurity response plan

Preparation is key to minimizing the impact of a cyberattack. Every horticulture business should have a cybersecurity response plan outlining:

- Immediate response steps: Isolating affected systems, assessing the extent of the breach and initiating backups.
- Incident reporting: Establishing protocols for notifying stakeholders, including employees, vendors and customers.
- System restoration: Ensuring backup recovery processes are in place and that operations can be restored swiftly.
- Legal and regulatory compliance: Understanding obligations for reporting breaches and potential liabilities.

The horticulture industry is not immune to cybersecurity threats and businesses must take proactive steps to safeguard their operations. By understanding common cyberattack tactics, enforcing robust security measures and investing in cyber insurance, greenhouse operators, garden centers and nurseries can significantly reduce their risk exposure. A strong cybersecurity framework protects not only financial assets, but also the trust and confidence of customers and vendors. In today's digital world, cybersecurity is a necessity, not an option. **GT**

Dan Zastava is the director of corporate underwriting and products for Sentry Insurance. Hortica is a brand of the Sentry Insurance Group.