withum

CASE STUDY

CYBER AND INFORMATION SECURITY

INTERNATIONAL FLOWER WHOLESALER AND DISTRIBUTOR GETS FULLY-INTEGRATED IT INFRASTRUCTURE

Discover how Withum's Cyber and Information Security Services Team was able to enhance and secure the IT environment of a U.S.-based flower company with international imports and exports while simultaneously streamlining business operations.

EXECUTIVE SUMMARY

Withum's Cyber and Information Security Services Team delivered a fully-integrated IT infrastructure that adheres to international data privacy laws and regulations for a U.S.-based wholesale flower grower and distributor. Through various IT assessments, walkthroughs and virtual CISO roles, Withum delivered the business with comprehensive IT security posture enhancements to help mitigate future cyber threats. The company now has a roadmap for the future and will enhance the IT security of international operations, anticipating aggressive growth in South America, in particular.

THE CLIENT

A U.S.-based wholesale flower grower and distributor with South American operations was experiencing significant year-over-year growth, quadrupling in size during a six-year period. Management knew that its internal technology and IT infrastructure would soon be unable to allow them to operate efficiently and securely in today's tech-driven business environment. Tapping into their existing relationship with Withum, the client chose the Firm's Cyber and Information Security Services Team, after an extensive RFP (request for proposal) process, to assess the company's current IT infrastructure and general IT security practices and look for opportunities to strengthen company-wide operations.

CASE BRIEF

CLIENT: Wholesale flower grower and distributer with international operations

STRENGTH: Quick and efficient at supporting rapid growth

CHALLENGE: Integrating business systems to support new international growth while meeting legal and security obligations

OPPORTUNITY: Provide the company with up-to-date security protocols and technology

OUTCOME: Enhanced IT infrastructure and cybersecurity processes and controls that scale as the business grows

With their rapid growth, management knew there were areas of vulnerability and opportunities for operational improvement that, if addressed properly, would streamline the company's operations and strengthen its scalability as the business continues to grow.

THE CHALLENGE

The flower wholesaler knew that holes existed in their current IT environment. Because of its substantial growth, many systems were not well integrated, technology was outdated and even running on old, near-obsolete systems. Although the business knew they were missing a cohesive, linked strategy and systems, it didn't have the internal resources necessary to properly assess their current IT infrastructure and cybersecurity processes and procedures.

Due to the fragile physical nature of flowers, time is money and operational efficiency is everything. Management knew that a secure IT infrastructure and efficient business operations were paramount in allowing the business to meet current market demands. These items were also necessary to be able to scale quickly and efficiently as the business continues to see growth.

The company faced an added challenge as the demand for flowers increased due to the COVID-19 pandemic. Management knew that in times of high demand and change the probability of an external threat or security breach remained just as high, or higher, than during times of normal business operations. Typically, when businesses are primarily focused on meeting their business obligations and delivering on their services, it is easier for foreign actors to successfully compromise companies because internal resources are preoccupied.

THE APPROACH AND SOLUTION

The IT and management teams knew their IT infrastructure and cybersecurity practices weren't at required levels and wanted a third party to help close their vulnerability gaps. Withum's Cyber and Information Security Services Team was the necessary partner who could assess their current general IT security practices and mitigate areas of vulnerability while streamlining their business operations. Withum's reputation, qualifications, experience and additional familiarity with South American laws and regulations made the Firm a perfect fit for the job.

Withum's Cyber Team took a multi-prong approach to assessing the flower wholesaler's current IT infrastructure and security operations.

STEP 1. Performed a threat and intel assessment. This Open Source Intelligence (OSINT) approach allowed Withum's Cyber Team to perform tasks such as dark web and database scans as well as other business intelligence tests. The OSINT report served as a foundational element in uncovering areas of vulnerability in the company's IT infrastructure.

STEP 2. Performed and in-depth technical assessment. This assessment included a focused penetration test. The company's IT Team shared areas of known weakness, enabling the Cyber and Information Security specialists to execute controlled attacking of internal systems. More time was spent on testing current IT processes than discovering areas of liability.

This process included Withum's Air$_4$Droid™ devices. Four devices were introduced into the IT environment to perform real-time cyber threat emulation and vulnerability scans. These devices also provided real-time feedback on phishing assessments, allowing the company to deploy necessary training to help lessen the probability of falling victim to future phishing attacks.

STEP 3. Performed a Virtual Chief Information Security Officer (vCISO) assessment. The vCISO assessment enabled Withum's Cyber Team to analyze the vulnerabilities and current infrastructure as well as programs and processes. The Cybersecurity specialists were able to create a long-term strategy for the flower distributor based on their business goals that would grow with them. Looking at each angle of the business in a vCISO role provided a holistic approach to solving the company's IT issues. The vCISO assessment assisted the flower business in applying and establishing better IT security processes for the company.

Acted as a short-term Virtual Chief Compliance Officer (vCCO) to ensure data privacy rules were appropriately followed. As a vCCO, Withum's Cyber Team enhanced the company's current IT security processes to provide an added layer of data protection.

THE RESULTS, ROI

By performing the OSINT assessment, operating in a temporary vCCO role, deploying AIR$_4$Droid™ devices and working with leadership across all areas of the organization, the flower wholesaler was able to close immediate gaps in their IT infrastructure and cybersecurity operations while having a plan for the future.

Withum's Cyber and Information Security Services Team:

- Identified database vulnerability issues and closed those gaps immediately.
- Eliminated inconsistent patching issues within the IT environment and created new processes and procedures to keep operations secure.
- Updated and implemented appropriate IT security controls that adhere to international data privacy rules and regulations.
- Optimized current WiFi and Bluetooth infrastructure at the distribution facility to create a fully-integrated network that also cuts out interference from neighboring businesses and international airports.
- Created a roadmap for future cyber security operation upgrades as well as a plan for upgrading IT systems, servers and cybersecurity processes and procedures in the company's South American locations.

The project allowed Withum to reduce risk and mature existing IT security systems and processes to make the business more cyber-secure and operationally efficient.

Matthew Ferrante | **T** (800) 470 0988 **D** (212) 537 9397 **wcyber.sales@withum.com**