withum

CASE STUDY

CYBER AND INFORMATION SECURITY SERVICES

LEADING IRRIGATION BUSINESS STRENGTHENS ITS BUSINESS POSITION THROUGH CYBERSECURITY

Learn how Withum's Cyber and Information Security Services Team transformed and aligned an irrigation company's IT technology to streamline short and long-term business objectives, strengthening its position in the market for future growth and M&A opportunities.

EXECUTIVE SUMMARY

A California-based, leading, family-owned landscape and irrigation company struggled with ill-advised selection and adoption of IT and business technologies. These solutions were also not in line with company objectives. Miscommunication between management and their IT service provider on proper business technology processes and procedures left the business vulnerable to cyberattacks. They turned to Withum as a trusted advisor to conduct an independent IT assessment, which uncovered dangerous flaws in their infrastructure. By delivering newly enhanced IT and security monitoring, the company has appropriate cybersecurity controls in place and its business prospects for future deals are brighter.

THE CLIENT

The client, a leading family-owned landscape and irrigation business based in Anaheim, California, has a footprint in the region for over 30 years with an estimated annual revenue of ~$200M USD and growing. Before engaging Withum, the client suffered a ransomware attack that paralyzed the business and affected the confidentiality, integrity and availability of the entire infrastructure. This cyberattack caused significant losses for the business, including an outage. Post-impact, the client's IT advisors were not overly alarmed.

CASE BRIEF

CLIENT: Leading, family-owned landscape and irrigation business based in California.

STRENGTH: Business continues to grow and expand.

CHALLENGE: IT Security Concerns and inefficiencies; poor productivity levels; technology not aligned to growth; regulatory and business objectives.

OPPORTUNITY: Create a simplified, secure, and modernized IT infrastructure.

OUTCOME: Reduced risk of data breaches, outages, regulatory violations, and much more; realignment and utilization of IT/IT Security framework to streamline services.

However, executive leadership felt that a third-party opinion was necessary to ensure remediation efforts were sufficient and the company's IT was on the right track. Since Withum was already providing services to the client and delivered on several other services, the Withum Trusted Advisor suggested that they look deeper into their IT infrastructure to provide an objective assessment.

THE CHALLENGE

The client acknowledged that they were concerned about cybersecurity; however, their IT service provider consistently reassured management that the environment was secure and moving in the right direction. Ownership was misled by their service provider and was in the dark about the IT environment – several issues existed such as a lack of a security program and documentation, inefficiencies, vulnerable platforms, licensing issues, overtaxed systems, failure to apply critical patches to systems, negligent and reckless password and system account handling, unauthorized and rogue assets, data privacy violations, among several other deficiencies. These vulnerabilities and issues positioned the client as the perfect target for crippling cyberattacks. Withum conducted a Threat Intelligence test to see what competitors, malicious actors, insurers and potential investors could see publicly and on the dark web. The cybersecurity specialists issued a confidential Withum Open Source Intelligence Report (OSINT Report) to the C-Suite. Although their IT service provider was resistant, an executive decision was made by management to move forward with a more in-depth assessment as a 'checks and balances' and 'trust but verify' approach.

THE APPROACH AND SOLUTION

Knowing Withum's Cyber and Information Security Team's prestigious and extensive expertise, the client was confident that Withum was the right firm to assess the state of their cybersecurity and IT technologies and provide appropriate recommendations based on the results.

As part of the engagement, Withum's Cybersecurity Team subsequently conducted a series of tests and assessments:

- Penetration testing of the virtual environment.
- Authorized hacking of the environment via the Withum e^3 Red Team™ service.
- Virtual Chief Information Security Officer ("vCISO") review of security controls.
- Virtual Chief Compliance Officer ("vCCO") review for data privacy and regulatory compliance assurance.

Withum's Cybersecurity Team identified serious flaws in the client's security and the overall IT infrastructure design. In fact, the cyber team was also able to hack and take full control over the environment. Additionally, Withum uncovered several vulnerabilities, some as serious as data privacy violations and unreliable or failing backups. Malicious cyber attackers could have paralyzed the business for prolonged periods of time.

During the assessment, it became clear that the client's IT infrastructure was inefficiently designed, insecure and lacked sufficient compliance controls necessary for a business of this scale. It became evident that the client's IT infrastructure was not aligned to current and long-term business objectives. This was not just a security issue, but an IT framework that simply did not fit the business. IT and technology are not 'one size, fits all'. It must be fitted to the business, for the business, and aligned to the market as a business enabler.

With the amount of IT vulnerabilities that existed, the misalignment of the IT infrastructure as a whole, and the cost of ad-hoc, piecemeal remediation efforts, the client agreed it was in their best interest to retain Withum's IT Managed Services with cybersecurity integration. These services included:

- remediation of their IT/IT security framework
- dark web scans
- continuous IT/IT security monitoring via Withum's Fusion Center, providing 24/7/365 IT/IT security support to ensure the business can maximize its return-on-investment for their IT/IT security investments.

Selecting Withum as their cybersecurity trusted advisor placed the client's business in a position of strength and growth, regardless of the inevitable storm. Withum enabled the client to focus on their business, not their IT and the ever-increasing threat landscape.

A threat landscape or a threat environment is a collection of threats to a particular area or business, with information related to that business's vulnerable assets, threats, risks, threat actors and observed trends.

The cyber team deployed nineteen Withum AIR$_4$Droid™ devices to deliver real-time remediation, validation, protection and monitoring of client's systems. Withum's AIR$_4$Droid™ devices provide intelligent identification, scanning, probing and mapping of an organization's network(s) devices and vulnerabilities, among other capabilities.

THE RESULTS

Realizing the need for strengthened cybersecurity, Withum's solution helps mitigate any new potential cyber threats against the organization. The client now receives real-time active and passive cybersecurity monitoring, alerts, auditing, incident response, secure backups, cyber forensics and reporting to a secure, personalized account through Withum's 24/7/365 Security Operations Center. By properly securing and structuring the IT infrastructure, monitoring the system with Withum Air$_4$Droids™ and streamlining the communication process, management and IT now operate on the same page with trusted intelligence.

The consolidation and streamlining of their IT infrastructure, as well as the enhanced security posture will return significant savings and risk aversion:

- Cyber-attack risk reduced from $8.19M (US national average of a data breach)
- Operational expenditure reduction of $200,000 per year (hardware, software, IT managment expenses)
- Reduction of IT power and resource consumption of over 75%
- Downtime monitoring introduced to the environment; uptime increased exponentially. Uptime valued at over $300 per minute

Withum's Cyber and Information Security Services strengthened the client's defenses and compliance posture and aligned their IT and business objectives moving forward. The engagement helped future-proof the company for M&A, making it appealing to investors for a buy-side or sell-side transaction.

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