The Balancing Act for Mid-Market Firms: Navigating Digital Growth and Security Hurdles

By Kevin Beasley, CIO, VAI

Increased competition and new regulatory requirements are increasing the tempo of digital transformation among mid-market companies.

In fact, Deloitte's 2023 Mid-Market Technology Trend report found that technology spending among this cohort is at its highest level since 2019.

However mid-market companies face cybersecurity challenges when it comes to their expanding digital footprints. It's hard to find the cybersecurity talent that businesses need to fend off ransomware attacks and manage software vulnerabilities. They are resource-constrained in other ways: with limited or non-existent recovery plans, and an absence of training for key employees.

"Cloud Enterprise Resource Planning (ERP) systems are a strong antidote to the cybersecurity maladies mid-market companies face. Here's why.

Ransomware and Evolving Threat Landscape

Ransomware attackers extorted at least $449.1 million from organizations in the first half of 2023 alone, according to a threat assessment from the Department of Homeland Security. While that number may be eye-popping on its own, what may be even more surprising to some is the complex economic environment that supports it.

Ransomware is big business. There are employees, managers, and executives in ransomware cartels. These criminal organizations conduct scams on their own, but they also license their service to other threat actors in exchange for a cut of the proceeds, a phenomenon known as “ransomware-as-a-service.” Threat volumes for all companies are extremely high, and the bad guys only have to win once, while security teams have to win every time.

And the effects of a ransomware attack can be disastrous.

The average business experiences a recovery period of 22 days before resuming operations following a ransomware attack, which frequently costs 50 times more than the ransom demand, DHS says.

Cloud ERP systems can offer a higher inherent degree of security due to their centralized updates and expert-managed security protocols. They eliminate the inconsistencies of individual end-point security measures by ensuring real-time, system-wide protection.

Cloud ERP systems serve as a lifeline in the high-stakes aftermath of a ransomware attack, by significantly reducing recovery time and costs. These systems offer robust data backups and redundancy measures, ensuring that businesses can restore operations quickly and efficiently without giving in to ransom demands.

They also perform the same function in the face of natural disasters and other business disruptions. By housing data in secure, remote servers managed by professionals with top-tier expertise in digital security, these systems mitigate the risk of local data breaches and physical server damage.

Simplifying the Talent Gap

There are, according to research, just 69 cybersecurity candidates for every 100 job openings in the field. Large companies struggle to hire, and often pay large salaries for talent. Mid-market firms can be shut out.

Cloud ERP systems allow companies to draw on the expertise of the ERP maker, and they can further expedite the integration of new security protocols and software updates. Instead of allocating resources to find scarce cybersecurity experts, these companies can rely on the robust security measures that come inherently with cloud-based ERP systems.

These platforms are equipped with automatic updates and are backed by a team of security experts from the provider, ensuring that the system is always up to date with the latest security standards and protocols. This not only alleviates the pressure on mid-market firms to compete for cybersecurity talent but also mitigates the risks associated with human error and insufficient in-house expertise.

The Digital Footprint

Two trends dominate in the digital evolution of the mid-market. In food and pharmaceutical distribution, for example, there's a push for traceability across the entire supply chain, from raw materials to the consumer and from farm to table. Technologies like blockchain and IoT are helping to meet those requirements. Among distributors of non-perishable hardgoods, the need for superb customer service amid competition from bigger, resource-rich competitors are pushing mobile technologies into the mix to streamline ordering and logistics processes.

All these digital tools can be a target-rich threat environment.

Cloud ERP is a reliable and resilient component of many mid-market business architectures because they help to integrate this expanding digital footprint into a single, comprehensive system. This centralized approach not only counters the skills gap in cybersecurity expertise but also provides a proactive defense mechanism against the ever-evolving threat landscape.

About the Author

As CIO of VAI, Kevin Beasley oversees both the corporation's technology strategy in conjunction with product development and the internal information technology initiatives that support the goals of the company. He has decades of ERP, SCM, and WMS consulting experience and extensive experience in the IT space. For more on VAI, please visit vai.net.