IT Focus: Cybersecurity

Dealerships helping customers protect digital assets

by: Brent Hoskins, Office Technology Magazine

In a world of constant cyberthreats, is your dealership working to help your customers mitigate the risks? The following profiles provide a brief look at three BTA member dealerships in terms of their common focus on providing cybersecurity. Perhaps the comments they share will provide you with some welcome insight.

Advanced Business Methods

Although it was founded in 1971 and has since grown to 111 employees working from seven locations in North Dakota and two in Minnesota, it was only last year that Advanced Business Methods (ABM) — offering Canon, Ricoh, Kyocera, HP and Lexmark imaging devices — entered the managed IT services business. Headquartered in West Fargo, North Dakota, ABM established the ABM Technology Group with the acquisitions of two IT companies — True IT and Millennium Systems. Today, the IT division accounts for 20 of ABM's employees and it has plans to expand its headcount.

ABM's managed IT services business has grown 217% in its first nine months, says Ben Nelson, vice president of the ABM Technology Group. He emphasizes the added pull-through opportunity for imaging devices. "In terms of our IT customers new to ABM, 90% of them will convert their MFPs to ABM," he estimates, adding that only about 6% of current ABM imaging customers will become IT services customers, too. However, he adds, 6% of ABM's 14,000 to 16,000 customers is not an insignificant percentage.

Nelson says ABM's IT sales strategy is to keep it simple. In fact, the dealership's motto is "Technology Simplified." He shares the three components of the ABM Technology Group's managed IT services offerings. "We have True Secure, our cybersecurity package," Nelson says. "Then, we have True Managed — managing your network, doing patch updates, backups, etc. And, finally, we have True Support, our help desk and break/fix side."

Looking at ABM's cybersecurity package in particular, Nelson says it serves to secure devices and mailboxes. "We do that with nine layers," he says. "This includes advanced threat protection, DNS [domain name system] security, endpoint detection and response, and antivirus. For mailboxes, we provide security awareness training, spam filtering, backup for their Microsoft 365 accounts, managed detection and response, and anti-phishing."

What is the biggest cybersecurity threat to companies? "It is always an employee," Nelson says, citing a recent example. "Two weeks ago, right after we implemented our security offering, an employee downloaded what he thought was an invoice from a customer. It wasn't an invoice. It started executing malware in the background. Our EDR system identified the software as suspicious, quarantined and killed the bot. Had our EDR not been in place, the outcome might have been disastrous. Instead of an entire company being down for days or weeks, one user lost productivity for a couple of days to scrub his machine."

Referring to them as "threat actors," those with nefarious intent are "casting wide nets," Nelson says. "Cyberterrorists are no longer targeting specific companies — they are going after vulnerabilities. They don't care what type of business you are in. They're just out phishing and if you click on something, they are in there and start looking around. They may be in there for months just monitoring your behavior. Perhaps it is: 'This guy is about ready to purchase a truck, and I'm going to wait until he is ready and then I'll ask for a wire transfer.'"

Such attacks are being exploited though the use of artificial intelligence (AI), Nelson says. "AI threats are up 658% in just the last three months," he says. "Threat actors are using AI to create material and threats, using it to their advantage. There are a lot of AI security tools that are being implemented, but the threat actors are just as fast at getting better with the use of AI."

The threat actors are most often overseas, Nelson says. "These are people making 10 cents a day in third-world countries," he says. "When they are successful with a ransomware attack and a company pays them a quarter million dollars to get its data back, the threat actor basically just won the lottery. Someone else sees that and thinks: 'If this guy can

do that, why can't I do the same thing?'"

Nelson adds that ABM's cybersecurity package is also helping customers address the high cost of cybersecurity insurance, noting that the key is ensuring the customer is able to effectively complete what is widely known in the insurance industry as the Tokio Marine Application. "With our secure IT deliverables, we help them check 100% of the boxes on the application," he says. "Our goal is to be able to get them the best coverage for the price — and adding our tools has proven effective with our clients when they are applying for cybersecurity insurance."

> "When they are successful with a ransomware attack and a company pays them a quarter million dollars to get its data back, the threat actor basically just won the lottery."
>
> 
>
> *— Ben Nelson*
> *Advanced Business Methods*

Altek Business Systems

Founded in 1991, Altek Business Systems is headquartered in Telford, Pennsylvania, with a second office in Marlton, New Jersey. The dealership, which offers Canon, Kyocera and Xerox imaging devices and has approximately 30 employees, began offering IT services 14 years ago. Six years ago, when Wilhelm Rebmann joined the dealership as chief technology officer, Altek expanded its IT services offerings. "We consciously decided that we were not going to have break/fix IT customers," he says. "Instead, today, if you are an Altek IT customer, you are fully managed."

The five-person IT department at Altek is profitable and growing, Rebmann says. "We are at more than a million dollars in managed customers," he says, noting that the number includes IT services, but also Altek's document management and VoIP sales. "Six years ago, we only had two or three customers that were fully managed. Today, we are at 50."

Altek offers base-level IT services, with advanced security services layered on top of that, Rebmann says. "We just started adding advanced security in the last couple of months," he says, noting that there has been an "amazing increase" in the need for cybersecurity. "Two years ago, about 90% of our job was to provide support and functional efficiencies and about 10% was security. About a year ago, it was 50/50. Now it's almost 80% security and 20% support. We're still doing the same amount of support. It's just that we're doing a ton more in terms of security."

To demonstrate IT vulnerabilities and provide educational opportunities, Altek uses a cybersecurity penetration test conducted by Galactic Advisors for prospects as part of the sales process and quarterly for existing customers. "In each test, the prospect or customer clicks on a white hat phishing link [referred to as 'ethical hacking'] on a few computers on their network and answers a few questions, such as 'Do you have phishing training? (Altek partners with INFIMA for the training),'" Rebmann says, noting that Galactic Advisors and Altek sign a nondisclosure of what is found as a result of the phishing link. "Galactic Advisors then prepares a report on the network's vulnerabilities [with specific information blocked out]. The report shows user passwords, passwords that are being reused and passwords that are also on the dark web. In addition, the test will look to see if it can find information containing Social Security numbers. All this information can be obtained in about 20 to 30 seconds with a single click."

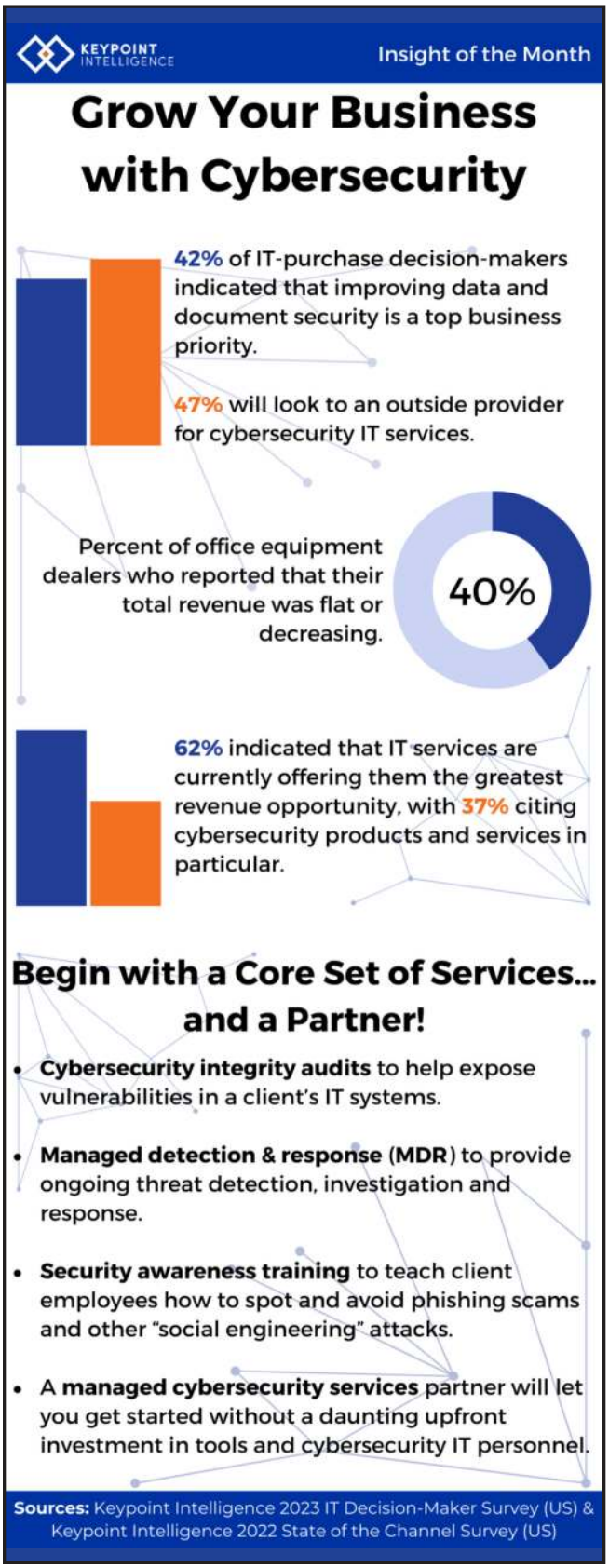
Rebmann says most prospects and customers are supportive of the penetration tests. "We haven't had a lot of pushback," he says. "We explain it up front and tell them it will allow us to see whether they have issues. Most think they are going to do great and have no issues. They are surprised by what is found. We can mitigate those issues easily once we start providing our cybersecurity services."

There are two primary reasons for more dealers to begin offering cybersecurity, Rebmann says. First, he says, cyberattacks are not going to go away and, so, the vulnerabilities will always need to be addressed. "The volume of attacks is increasing drastically," he says. "Unless a company disconnects its network from the internet and does all of its work internally, cybersecurity services are going to be necessary."

The second reason for office technology dealerships to pursue cybersecurity is the advantage they have over IT-only managed services providers (MSPs), Rebmann says. "I like being an IT person in the MFP world," he says. "I see the advantages of the sales teams and the structure of the dealerships. In contrast, MSPs may attempt to hire salespeople occasionally. Usually, they just get referrals — if they are lucky. Dealerships have a huge advantage. They've had the sales process down for years and they are good at it. So, there are tons of opportunities for them."

C3 Technology Services

In 1994, Copier Products Group, based in Santa Ana, California, was established as a managed print services company. In 2011, it transformed into C3 Technology Services, an IT services and office technology company. "'C3' means 'client-centered consulting,'" says Tony Sanchez, president



> "I see the advantages of the sales teams and the structure of the dealerships ... They've had the sales process down for years and they are good at it. So, there are tons of opportunities for them."
>
> *— Wilhelm Rebmann*
> *Altek Business Systems*

of the dealership. "We consult our clients. We want to listen to them and, as industry experts, give them our feedback in terms of their office technology."

While C3 offers Canon and Sharp imaging devices, Sanchez describes C3 as "vendor agnostic," emphasizing that the company also regularly accesses other brands through distribution channels. In addition, C3 offers managed IT services, VoIP phone systems, smart boards, laptops and touchscreen monitors.

Today, seven of C3's approximately 35 employees are members of the dealership's managed IT services team. "We started our team with one manager," says Davis Tran, vice president of operations. "We have since brought in additional skill sets as we have grown our IT services portfolio. When we started, we were selling help-desk support, offering customers a hybrid solution or full-blown IT support, with a C3 IT person doing everything for the customer."

Over time, as the IT department continued to develop, "we started figuring out what is in scope and what is out of scope — what's going to make us more money versus what is going to make us bleed," Tran says. "We didn't want to keep adding new employees as we add new contracts. So, today, with everything trending toward cloud services, we are doing more subscriptions versus providing a person who does everything IT related for our customers."

Among C3's subscription-based offerings are various tools providing cybersecurity. "The key is to have layers and layers of security," Sanchez says, noting that layers of security tend to redirect hackers to less protected targets. "They are going to say, 'Oh, this company has these different layers of security, we're going to move on.' They want 'easy pickings,' so if they can't get in with a cursory attack, they're going to move on to the next target."

At C3, the approach, in part, is to identify vulnerabilities and educate end users on how to mitigate cyberattacks, in addition to implementing layers of cybersecurity, Sanchez says. He shares some of the questions that need to be asked

of prospective customers. "'You've got to have layers of defense,'" he says. "'Do you have the right infrastructure in place? Do you have a firewall that is up to date? What happens if people forget to update their software or their license has expired?' It is sort of like driving a car. For your safety, you better have your seatbelts on."

One of the methods C3 uses to identify vulnerabilities is "phishing campaigns where we try to catch them opening a phishing email in the controlled world before it happens in the real world," Tran says, noting that only the executives at customer locations know about the campaigns. "We make the emails trendy. For example, during the COVID-19 pandemic, the email would say something like: 'Click here to get a test kit.'" Someone always clicks on the link, Sanchez says. He adds: "Even the people who know we're going to do this — the executives — will click on it."

> "The key is to have layers and layers of security. They are going to say, 'Oh, this company has these different layers of security, we're going to move on.' They want 'easy pickings' ... "
>
> — *Tony Sanchez*
> *C3 Technology Services*

Ultimately, the phishing campaigns train workers to recognize suspect emails and know what to do — "alert the IT staff, place the email in a junk folder or mark it as phishing," Tran says. He adds that C3's cybersecurity training doesn't stop there. The dealership also partners with INFIMA for training. "There is video training and quizzes. It also allows us to see the behaviors within the company. Who are the employees who skip the training? Guess what, they are often the ones who click on the phishing campaign emails." ■

Brent Hoskins, executive director of the Business Technology Association, is editor of Office Technology magazine. He can be reached at (816) 303-4040 or brent@bta.org.