MSP & MSSP Industry Notes

Sponsored by

Arcoa Group

Why partnering with ARCOA makes sense

Electronics Recycling is an important and profitable part of the IT asset lifecycle, but it can be overwhelming with all you already do, varying state regulations, and the limited resources at hand. That's where ARCOA comes in. When you partner with ARCOA, you get all the benefits of a big company without any of the capital investment. We've been doing this since 1989 and have the expertise, certifications, and nationwide resources to get the most for all your clients' retired IT assets. Plus, positioning your clients as environmental stewards not only elevates their appeal to consumers, it meets government requirements and avoids fines.

What partnering with ARCOA looks like

Our role is to make it easy for you to bring more value to your clients. We work with you to help stretch your clients' IT budget by reducing the total cost of ownership of their electronics. We're experts at identifying and implementing the solutions your clients need for the end-of-use remarketing, recovery, and recycling of their technology assets. The sooner you involve ARCOA, the sooner you and your clients will see better results.

IBM Announces Acquisition of Cloud Implementation Application Transformation & Managed ...

- IBM Corp., announced on Tuesday it has acquired Nordcloud, a European cloud implementation, application transformation, and managed services provider
- acquisition comes just days after IBM announced it acquired **Expertus Technologies Inc.,** a Canadian Fintech company that assists clients with processing over $50 billion in transactions per day
- Nordcloud claims to be a European leader in public cloud infrastructure solutions and cloud-native application services

Sirius Captures No. 1 Ranking of Top Diversified Managed Services Providers

- Sirius Computer Solutions, Inc. (Sirius), a leading national IT solutions integrator, ranked first in the inaugural 2020 Channel Futures 2020 NextGen 101
- Champion Solutions Group, Inc., a newly acquired Sirius company, also made the list.
- Florida-based Champion ranked 31st on the NextGen 101
- The 2020 MSP 501 and NextGen 101 lists are based on data collected by Channel Futures and its sister site, Channel Partners. Data was collected in 2020

Atos confirms expertise in Cloud services with renewed recognition as a Microsoft Azure Expert ...

- Atos announced that it has successfully renewed its status as Microsoft Azure Expert Managed Service Provider (MSP), for the 2nd consecutive year
- Atos is one of less than 100 Microsoft Azure expert MSP partners worldwide and was amongst those that qualified early in July 2019

Konica Minolta Receives Four BLI Awards from Keypoint Intelligence

- Konica Minolta Business Solutions U.S.A., Inc. (Konica Minolta) announced it has received four prestigious Buyers Lab Awards from Keypoint Intelligence
- BLI PaceSetter Award in Healthcare
- BLI 2021 Pick and Outstanding Achievement Awards
  - Outstanding Cost Accounting & Recovery Solution: Konica Minolta Dispatcher Paragon
  - Outstanding Achievement in Innovation: Return to Work
  - BLI 2021-2022 PaceSetter in Hybrid Workplace

Pharos updates solution

- Now offering version 5.3 of its Blueprint Enterprise solution
  - Provides administrative improvements
  - Touchless printing via Pharos Print mobile app
  - Mobile QR Code print release configuration
  - Sentry Print secure print support for Konica Minolta, Xerox and HP devices

Employees now more likely to expose data - Study conducted by Code42 Security

- 85% of employees are more likely to leak files today than before pandemic
- 76% of IT security leaders say their organizations have experienced one of more data breaches since work from home started
- 59% = insider threats will increase in next 2 years

- 54% = do not have formal insider risk response plan
- 40% = do not assess how effectively their technologies mitigate insider threats

Study on government use of paper - Research conducted by Center for Digital Government

- Survey of state and local government leaders
- 52% = paper documents make up 50% or more of initial records
- 68% = indicate eliminating paper is moderate to very urgent
- 70% = need for digital documents have increased due to pandemic
- 70% = accessibility on constituent-facing applications is either important or extremely important

Square 9 launches new services

- Square 9 Software, maker of DM and ECM solutions, and headquartered in New Haven, CT, introduced GlobalCapture Cloud Transformation Services
- Provides an end-to-end secure platform for digital transformation in the cloud
- Users have a complete cloud solution to capture, store and automate business processes

Boston Managed IT Outsourcing Cloud And VoIP Security Solutions Updated

- Newly updated IT outsourcing and managed IT services have been launched by the team at IT Management Solutions.
- Work with clients from Boston, New England

Ntiva and Southfield Capital Announce the Strategic Acquisitions of Forget Computers and Netlink ...

- Southfield Capital, announced that Ntiva, Inc., ("Ntiva" or the "Company") has completed the acquisitions of Forget Computers and Netlink Systems
- Transactions represent Ntiva's ninth and tenth acquisitions in the U.S., reinforcing the Company's continued growth in the MSP market
- Forget Computers, based in Chicago, IL, is recognized as the top-rated Apple Technology experts in the Midwest and have focused solely on helping organizations support their macOS and iOS users
- Netlink Systems, a provider of managed IT services based in Queens, New York, adds direct access to Manhattan and the surrounding metropolitan area

[AuthBridge, India's largest Authentication Technology Company unveils electronic signature ...](#)

- AuthBridge Research Services Private Limited, India's largest authentication technology company, announced the launch of its new electronic signature solution, SignDrive, a cloud-based document management solution
- SignDrive is built on AI-driven optical character recognition (OCR) and the image recognition technology, and comes with an in-built signer verification
- SignDrive combines AuthBridge's AI-powered verification technology with MSBDocs' automated document processing capabilities and offers a hybrid signature solution which includes electronically generated signatures

Cybersecurity Updates

- The federal Cybersecurity and Infrastructure Security Agency (CISA) reported a large scale hacking incident involving government agencies and organizations that use SolarWinds supply chain software.
  - "grave risk" to federal, state and local government networks
  - Symantec has identified infections on over 2,000 computers at more than 100 of its customers
- Attackers delivered malware to possibly thousands of organizations in the U.S.
- The FBI is reporting that the Wizard Spider hacking group of Russia is using Ryuk ransomware to extort $61 million in ransom from US healthcare firms.
- Colbi Trent Defiore was sentenced to 3 years in prison for stealing PHI to resell while working for a Medicare enrollment company in Louisiana.
- ThreatPost magazine reports that Microsoft Office 365 credentials are under attack by fax alert emails.
  - Email impersonates eFax to coerce users to click on attached document to unleash malware.
- Armis Security published report that 97% of devices affected by the Urgent/11 security vulnerabilities have not yet been patched
  - 80% of impacted devices are still vulnerable to attack
  - Relates to CDPwn flaws in the devices that use Wind River VxWorks code
  - (could include printers and MFPs)
- Weslaco Independent School District of Weslaco, TX notified an unknown number of students that their info may have been exposed after ransomware attack.

- Researchers announced that they have found a way to turn RAM chips into WiFi cards to steal data from computers.
  - Malicious code could be planted by attackers to manipulate the electrical current inside the RAM card in order to generate electromagnetic waves with frequency consistent with WiFi signal spectrum
- Taylor Made Diagnostics of Newport News, Virginia notified an unknown number of patients that their PHI was exposed after ransomware attack.
- Apex Laboratory of Long Island, NY and satellite in Florida notified an unknown number of patients that their PHI was exposed after ransomware attack.
- The U.S. Treasury and Commerce Department announced that Russian hackers broke into network and monitored staff email for months.
- The Jersey City Municipal Utilities Authority of New Jersey notified an unknown number of customers that their info may have been exposed after ransomware attack.
- The City of Independence, Missouri notified an unknown number of citizens that their info may have been exposed after ransomware attack.
- University Hospital of Augusta, Georgia reported that it is turning away 20% of all incoming emails due to security risks
  - Averaging 550 cyber attacks per day
- The City of Dade City, Florida notified an unknown number of citizens that their info may have been exposed after ransomware attack.
- The Great Neck Yeshiva High School of New York notified an unknown number of students that their info may have been exposed after cyber attack.
- Moderna Pharmaceuticals reported that hackers were able to access COVID-19 vaccine data.
- The Wall Street Journal reported that on December 14th, Google had an outage which impacted Gmail, G Suite apps and other services.
- Spotify notified an unknown number of customers that their info may have been exposed during recent data breach.
- Twitter was ordered to pay a $544,600 fine to the EU related to recent data breach.
  Helena Public Schools of Montana notifies some employees after burglar snatched USB with their time sheets.
- Meharry Medical College in Nashville, TN, notified 20,983 patients that their PHI was exposed after an email phishing attack
- MEDNAX Services Inc., headquartered in Sunrise, FL, is a provider of revenue cycle management and other administrative services to its affiliated physician practice groups that notified an unknown number of patients that their PHI was exposed after email phishing attack.

- GenRx Pharmacy, headquartered in Scottsdale, AZ, notified an unknown number of patients that their PHI may have been exposed after ransomware attack.
- The Pascagoula-Gautier School District in Mississippi notified 7,000 students that their info may have been exposed after ransomware attack.
- The Gardiner Public School District in Montana notified 200 students that their info was exposed after ransomware attack.
- Avast Security reported that 3 million users are believed to have installed 15 Chrome and 13 Edge browser extensions that contain malicious code.
  American Bank Systems, a document management company headquartered in Oklahoma, is being sued by its banking customers when their data was exposed during a breach.
-

Cybersecurity Updates

- The PHI (protected health information) of more than 16 million **Brazilian COVID-19** patients was exposed a hospital employee uploaded a spreadsheet on GitHub
- **Spamhaus** Security reported that more than fifty networks in the North American region suddenly burst to life after being dormant for a long period of time o organization is focused on tracking spam, phishing, malware, and botnets
  - noticed last week that 52 dormant networks in the ARIN (North-America) area were resurrected concurrently
  - each of them has been announced by a different autonomous system number (ASN), also inactive for a significant period of time

- o chances are almost zero for 52 organizations to suddenly come back online, all at once, although (a rare occurrence as well) some organizations might resurface after taking their network offline for a while.
- The **New York City Bar Association and the Chicago Bar Association** have both reported data breaches this year, according to reports filed with the Maryland attorney general's office.
- **Cadwalader, Wickersham & Taft Law Firm** reported a data breach incident to Massachusetts state officials.
- **Timothy Dalton Vaughn**, 22, whose online aliases included "WantedbyFeds" and "Hacker_R_US," of Winston-Salem, North Carolina, was sentenced by United States District Judge Otis D. Wright II to 95 months in federal prison
  - o The well-known hacker pleaded guilty to one count of conspiracy to convey threats to injure, convey false information concerning use of explosive device, and intentionally damage a computer; one count of computer hacking; and one count of possession of child pornography.
- **HP Inc.** released its 2021 predictions on **security threats:**
  - o human-operated ransomware, thread hijacking, unintentional insider threats, business email compromise, and whaling attacks – are set to increase in the next 12 months.
  - o "We can expect to see hackers identifying and taking advantage of any holes in processes that were created, and still exist, after everyone left the office."
  - o "if attackers are successful with destructive attacks on home devices, remote workers won't get the luxury of having someone from IT turning up at their door to help remediate the problem."
  - o "innocent actions – such as reading personal email on a company machine – can have serious consequences."
  - o "What we'll see is a rise in ransomware-as-service attacks where the threat is no longer the 'kidnapping' of data – it's the public release of the data."

  - o "The rise of 'double extortion' ransomware, where victim data is exfiltrated before being encrypted, will particularly hurt public sector organizations, who process all manner of personally identifiable information."
  - o "Even if a ransom is paid, there is no guarantee that a threat actor won't later monetize the stolen data."
  - o **One of the most at-risk verticals in 2021 will be healthcare**. "Healthcare has been a perfect target – society depends on it and these organizations are typically under-resourced, change-averse and slow to innovate"

- **Ardit Ferizi,** a computer hacker serving 20 years for giving ISIS personal data of more than 1,300 U.S. government and military personnel, has been granted compassionate release because of the coronavirus pandemic o will be placed in ICE custody for prompt deportation to Kosovo
- Ryan S. Hernandez, a computer hacker from Palmdale, CA, had pleaded guilty to stealing confidential **Nintendo** files o stole confidential information about popular video games, gaming consoles and developer tools
- **IBM** is reporting that unknown hackers are launching malware attacks on the "cold chain" of refrigerated vaccine distribution o urging those who are involved in shipping, storing, refrigerating, and delivering COVID-19 vaccines to beef up their security
    - o Many of the attempts involve emails impersonating an executive of a China-based biomedical firm whose contract attachment steals user credentials.

- The **Wall Street Journal** is warning drugmakers in the U.S., that they are being targeted by North Korean hackers o Hackers are looking to steal info on COVID-19 vaccines, treatments

- **Liv-On Family Care Center** of St. Paul, Minnesota reported that it was the victim of a robbery that may have exposed the protected health information of 1,580 people.
- **Methodist Hospital of Southern California** (MHSC) notified patients of a data breach involving third-party technology vendor Blackbaud.
- **Chesapeake Regional Healthcare** of Virginia notified 23,000 patients that their PHI was exposed after data breach against its fundraising and data hosting vendor, Blackbaud.
- **Advantech** of Irvine, CA reported that its confidential company info was posted to the Dark Web after a ransomware attack.
- **Gardiner Public Schools** of Montana notified an unknown number of students that their info was exposed after ransomware attack.
- **Beth Israel Deaconess Hospital** of Massachusetts reported that Zaosong Zheng, 30, was detained at Boston Logan Airport after CBP agents discovered 21 vials of cancer cells in his suitcase apparently stolen from hospital

- **Huntington City School District** of Alabama notified an unknown number of students that their info was exposed after a ransomware attack.
- **Stuller Jewelers**, headquartered in Lafayette, LA, notified an unknown number of customers that it was hit by a cyberattack.
- **NTreatment,** headquartered in San Francisco, CA, which manages PHI for doctors and psychiatrists, left 109,000 records exposed to the internet because one of its cloud servers wasn't protected with a password.
- **ZDNet magazine is reporting that a** hacker is selling access to the email accounts of hundreds of C-level executives o Access is sold for $100 to $1500 per account, depending on the company size and exec role.

- **McLeod Health** of South Carolina is notifying an unknown number of patients that their PHI was exposed after email phishing attack
- **AspenPointe,** a Colorado mental health services provider, notified an unknown number of patients that their PHI was exposed after ransomware attack.
- **Fairchild Medical Center** of Yreka, CA notified an unknown number of patients that their PHI was exposed after ransomware attack.