

January 24th, 2021

MSP & MSSP Industry Notes

Sponsored by



REMARKET • RECYCLE • RELOCATE
ThinkARCOA.com

[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.

[CTS Acquires ClearSky Technologies to Create a Comprehensive Offering of In-building Wireless ...](#)

- Communication Technology Services, a U.S. provider of in-building and campus wireless solutions, has acquired ClearSky Technologies, based out of Orlando, Florida
- The wireless industry is seeing two significant shifts - the need for greater indoor cellular coverage for mission critical applications and the ability for enterprises to deploy their own private LTE and 5G networks
- Acquisition provides Communication Technology Services a foundation of network solutions and expertise that is critical to the successful deployment of private LTE and 5G networks



REMARKET • RECYCLE • RELOCATE
ThinkARCOA.com

[Lexington IT firm acquires Ohio firm, expands into region](#)

- Reported on Wtvq.com
- NetGain Technologies, a managed IT services provider in the Midwestern and Southeastern U.S., has acquired Arnet Technologies and LK TECH
- Employees of both Arnet Technologies and LK TECH will join the NetGain team

[Thrive Acquires Apex IT Group](#)

- [Thrive](#), a provider of NextGen Managed Services, has acquired [Apex IT Group](#), a leader in IT technology managed solutions for companies in the Greater Philadelphia region
- Establishes Thrive's significant presence in the Mid-Atlantic corridor by expanding their Cloud & Cyber Security focused NextGen platform into the Apex IT client base
- Apex IT Group, headquartered in Mount Laurel, New Jersey, delivers IT managed services
- Apex IT Group will be a founding staple of Thrive's Mid-Atlantic region, overseen by Jason Shirdon, EVP & Regional General Manager, and formerly the President of EaseTech, a Columbia, Maryland MSP that Thrive acquired in late 2019

[etherFAX offers Direct messaging connector](#)

- etherFAX, headquartered in Holmdel, NJ, announced new DirectFax solution enables healthcare organizations to send and receive PHI directly to applications with end-to-end encryption
- etherFAX is provider of cloud-based fax server solutions
- Announced it won contract for new solution from Starling Physicians, which has 30 offices across Connecticut

[Quocirca report on print security](#)

77% of organizations surveyed reported that printing will be a very important or critical aspect of their business in next 12 months

- 64% experienced print related data losses in 2020
- Average cost of data loss of \$1.6 million
- 78% will be increasing print security solution spending in 2021
- 45% will go to their managed IT security services vendor for help with print security
- Only 15% trust their MFP/printer vendor for print security solutions



REMARKET • RECYCLE • RELOCATE
ThinkARCOA.com

[Importance of print security article](#)

- Published by The Imaging Channel magazine
In past 6 months, 2/3's of organizations have experienced data losses due to insecure printing practices
- 40% of IT decision-makers turn to their managed security service provider for print security advice
- Microsoft stated that 44% of hacking targets were in the information technology sector, including equipment (printer/MFP) providers
- Printers/MFPs are some of the most neglected devices on a customer's network when it comes to data security
 - Cybercriminals are aware of this and often target printers/MFPs for that reason
- The very remote monitoring and management technology that manage print services providers rely on, can also be source of security risk
- DCA (data collection agent) could be transformed into a silent and effective command/control attack vector for cybercriminals

[Fujitsu launches ScanSnap iX1600 and iX1400 scanners](#)

- Reported on betanews.com
- New iX1600 and iX1400
- iX 1600 has 4.3" LCD display and Wi-Fi
 - USB connect
 - Mac and Windows compatible
 - Uses ScanSnap software
 - iX1600 simplex scan speed of 40 ipm, duplex at 80ipm
 - Both will retail for under \$500

[Expereo certified as Advanced partner of Cisco's Cloud and Managed Services Program](#)

- Expereo, has been certified as an Advanced partner of Cisco's Cloud and Managed Services Program (CMSP)
- Expereo now a part of Cisco's world-wide Advanced partners
- Expereo is a provider of managed network solutions, including Global Internet connectivity, SD-WAN, and Cloud Acceleration services



REMARKET • RECYCLE • RELOCATE
ThinkARCOA.com

[The future of print in the digital workplace – Global Market Insight Study](#)

- Reported on itweb.co.za
- Digitization is also set to accelerate
- Print simply is not going to disappear any time soon
- “The ‘less-paper’ office is more likely than the paperless office”
- 78% say printing is important to their daily business
 - dropping to 64% that expect it will still be important in 2025

[Global PC shipments increase](#)

IDC reports that sales are up 26.1% during last quarter

- Reached a total of 91.6 million units
- Growth fueled by work from home and remote learning during pandemic
- Top manufacturers include:
 - Lenovo of China
 - HP
 - Dell
 - Apple
 - Acer

[Toshiba partners with Barracuda](#)

- Barracuda Networks, headquartered in Campbell, CA, is supporting the development of Toshiba’s global managed IT services blueprint
- “We have seen a lot of print companies that have been acquiring security centric or security capable managed service providers, so that they can go and provide more services to their customers, and they have proven to be extremely successful. I think we will see more and more organizations looking to see how they can change their focus, how they can do more for their customers, how they can retain their customers, how they can find new customers, and we are well positioned to help them do that.”, stated Jason Howells, VP of Barracuda
- Has also provided Toshiba’s printer/MFP division with ongoing marketing tools and support, including access to partner portal
- Is now running weekly training sessions for sales force
- Portfolio of security products including email, network, application, cloud, as well as managed services and data protection



REMARKET • RECYCLE • RELOCATE
ThinkARCOA.com

Cybersecurity

- ZDNet magazine now reports that 50% of hacking attacks on healthcare industry involve ransomware.
- The federal government announced that the year 2020 set a record for number of breaches in the U.S. healthcare industry.
- Socialarks, a social media management company, exposed 400 gigabytes of personal info from 214 million users due to an unsecure online database.
- President Donald Trump officially signed HR 7898 into law on January 5, 2021. The HIPAA
 - Safe Harbor bill amends the HITECH act to require the Department of Health and Human Services to incentivize best practice cybersecurity for meeting HIPAA requirements.
 - The legislation directs HHS to take into account a covered entity's or business associate's use of industry-standard security practices within the course of 12 months, when investigating and undertaking HIPAA enforcement actions, or other regulatory purposes.
 - requires that HHS take cybersecurity into consideration when calculating fines related to security incidents
 - required to decrease the extent and length of an audit, if it's determined the impacted entity has indeed met industry-standard best practice security requirements.
 - "this provision serves as a positive incentive for health providers to increase investment in cybersecurity for the benefit of regulatory compliance and, ultimately, patient safety,"
- A global law enforcement operation has taken down DarkMarket, which Europol describes as the world's largest underground marketplace of illegal goods on the dark web.
- DarkMarket has generated \$170.2 million in revenue by selling drugs, malware, credit cards and more
 - arrested a 34-year-old Australian alleged to have operated DarkMarket
 - also shuttered 20 servers used to host the illicit market located in Moldova and Ukraine
 - DarkMarket had more than 500,000 users, including 2,400 actively selling content, resulting in more than 320,000 transactions
- Rogue malware that can hack into an Android-based smartphone is up for sale on the Dark Web for as little as \$29.99
- Leon Medical Centers of Florida notified an unknown number of patients that their PHI was exposed after ransomware attack



REMARKET • RECYCLE • RELOCATE
ThinkARCOA.com

- Promutuel Insurance company notified 630,000 customers that their info was exposed after being posted online by a ransomware hacker.
- Banner Health, headquartered in Phoenix, AZ, announced it has agreed to pay \$200,000 to settle allegations of not providing patients with timely access to their PHI.
- Check Point Cybersecurity announced that its research shows that 43% of all email phishing attempts are attempting to pass themselves off as messages from Microsoft.
- Wall Street Journal reported that the TikTok app is exploiting a loophole to collect unique identifiers from millions of Android-based smartphone users and provide to Chinese government.
- Ring, the video doorbell company, notified an unknown number of customers that their info was exposed after a security flaw was discovered.
- Clearfield County government of Pennsylvania notified an unknown number of citizens that their info may have been exposed after ransomware attack.
- Beebe Medical Foundation of Lewes, Delaware notified an unknown number of patients that their PHI was exposed after a ransomware attack.
- Stormont Vail Health of Topeka, Kansas notified an unknown number of patients that their PHI may have been exposed after an employee illegally shared website access to outsiders.
- The Puget Sound Educational Service District notified an unknown number of students in King and Pierce counties of Washington, that their info may have been exposed after ransomware attack.
- Clark Hill Law Firm, headquartered in Detroit, MI, notified an unknown number of clients that their info may have been exposed after cyberattack.
- United Nations Environmental Program notified 100,000 people that their info may have been exposed after cybersecurity incident.
- Start Skydiving of Middletown, Ohio notified an unknown number of employees and customers that their info may have been exposed after being illegally accessed by a former employee.
- Galstan & Ward Family and Cosmetic Dentistry of Suwanee, GA notified 10,759 patients that their PHI was exposed after ransomware attack.
- Gastroenterology Consultants Ltd. of Nevada notified an unknown number of patients that their PHI was exposed after ransomware attack.
- Golden Gate Regional Center of San Francisco, CA notified 11,315 patients that their PHI was exposed after ransomware attack.
- Taylor Made Diagnostics of Virginia notified 3,464 patients that their PHI was exposed after ransomware attack.
- Warren-Washington-Albany ARC of New York notified 1,000 patients that their PHI was exposed after ransomware attack.



REMARKET • RECYCLE • RELOCATE
ThinkARCOA.com

- New Jersey Dental Hygienists' Association notified 160,000 patients that their PHI was exposed after ransomware attack.
- Reconstructive Orthopedic Center of Houston, TX, notified an unknown number of patients that their PHI was exposed after ransomware attack.
- Paramount Dental Studio of Huntington Beach, CA notified an unknown number of patients that their PHI was exposed after ransomware attack.
- Coldwater Orthodontics of Michigan notified an unknown number of patients that their PHI was exposed after ransomware attack.
- Delta Dental Plans Association of Illinois notified an unknown number of patients that their PHI was exposed after ransomware attack.
- All About potential Family Chiropractic of South Dakota notified an unknown number of patients that their PHI was exposed after ransomware attack.
- Crozer-Keystone Health System of Pennsylvania notified 6,863 patients that their PHI was exposed after ransomware attack.
- Capcom Video Games notified "thousands" of customers that their info was exposed after ransomware attack.
- Pitkin County government in Colorado notified an unknown number of citizens that their info was exposed after cybersecurity incident.
- Ronald McDonald House Charities, headquartered in Chicago, IL, notified 18,000 guests that their info was exposed after ransomware attack.
- Excellus Health Plan, Inc., headquartered in Rochester, NY, has agreed to pay \$5.1 million to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and to implement a corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules related to a breach affecting over 9.3 million people.
- Gainwell Technologies, headquartered in Conway, Arkansas, announced that someone may have gained unauthorized access to 1,200 participants' information in Wisconsin's Medicaid program.

Find out why so many **service providers** are choosing us as their **distributor of choice.**

Your Best Source!

