August 2nd, 2020

MSP & MSSP Industry Notes

Sponsored by

Arcoa Group

ARCOA Group is here to help you successfully manage your IT Asset Disposition process. We help you recover value from retired electronic equipment through responsible methods of reuse and recycling. We ensure proper handling of assets which may contain data, while being environment stewards for assets that have no reuse value and are headed for recycling. We've built a robust de-manufacturing process to offer additional options for asset value recovery by disassembling equipment for commodity grade materials, which can be diverted from landfills and be used to create new base materials.

Laserfiche Spark Invites Change-Makers to Reimagine the Digital Workplace

- Announced registration is open for Laserfiche Spark, a free video broadcast showcasing digital transformation tools and trends and the latest developments in Laserfiche software
- Under the theme "Be the Change," Laserfiche Spark will present strategies for innovating and adapting to new ways of working
- Laserfiche Spark will be broadcast twice on Aug. 19, 2020, from 10-11:30 a.m. EDT and from 2-3:30 p.m. PDT

New Hampshire's Department of Labor Partners with ImageSoft to Renovate 20-Year-Old ...

- Approximately 50 percent of the NH DOL staff are working remotely amidst the Coronavirus pandemic

- Currently in phase two of the discovery stage, the NH DOL is expected to be live with its digital OnBase solution in March 2021

Onix Achieves the Managed Services Provider Status in the Google Cloud Partner Advantage ...

- Announced that it has achieved the Managed Services Provider status in the Google Cloud Partner Advantage Program
- Headquartered in Lakewood, Ohio, Onix serves its customers with virtual teams in major metro areas, including Atlanta, Austin, San Francisco, Boston, Chicago and New York. Onix also has Canadian offices in Toronto, Montreal and Ottawa

Trustwave Positioned as a Leader in Global Managed Security Services

- Announced that the company was named a Leader in the latest Forrester Research, Inc. evaluation of global managed security service providers
- The Forrester Wave™: Global Managed Security Services Providers (MSSPs), Q3 20201, included 15 vendors in the assessment who were evaluated on 26 individual criteria grouped into three high-level categories including current offering, strategy, and market presence
- The Trustwave Fusion platform, a cloud-based cybersecurity platform, serves as the cornerstone for the company's managed security services
- Trustwave (trustwave.com) is a cybersecurity and managed security services provider

Ascend Technologies Acquires Infogressive

- Announced its merger with **Infogressive, Inc.**, a provider of cybersecurity solutions
- Transaction was facilitated by **IT ExchangeNet** (ITX), a leading mid-market mergers and acquisitions firm specializing in the sale of MSSPs, MSPs, and Microsoft channel partners
- The combined organizations will have over 150 U.S.-based technical and security professionals, with offices in Chicago, Illinois, and Lincoln, Nebraska

Offensive Security Acquires Open Source Security Training Project VulnHub

- Announced it has acquired open source security training resource hub VulnHub
- Acquisition is part of OffSec's ongoing mission to provide practical training content to aspiring cybersecurity professionals
- VulnHub is an open source, continually updated catalog of IT assets that are legally hackable, breakable, and exploitable by design
- All VulnHub content will remain available for free in keeping with OffSec's commitment to open source

Qualys Acquires Software Assets of Spell Security

- Announced it acquired the software assets of Spell Security, an endpoint detection and response start-up
- Further strengthens Qualys' security and threat research, advances endpoint behavior detection capabilities
- Spell Security employees have joined Qualys, including founder Rajesh Mony as CTO, Malware Detection Solutions

CSPi Technology Solutions Recognized on CRN's 2020 MSP500 List

- Announced today that CRN®, a brand of The Channel Company, has named it to its 2020 Managed Service Provider (MSP) 500 list in the Security 100 category.
- This annual list is divided into three categories: the MSP Pioneer 250 who are focused primarily on the SMB market; the MSP Elite 150, large data center-focused on- and off-premises; and the Managed Security 100 made up of off-premises-focused, cloud-based IT security services
- The full 2020 MSP500 can be viewed online at www.crn.com/msp500.

BDO Launches Athenagy™—The New Business Intelligence Platform for Managed Services

- Announced the launch of Athenagy™, its proprietary business intelligence platform for legal professionals

- Designed to integrate with a highly secure, customized Relativity®One environment

Xamin's Latest Whitepaper Urges Financial Institutions to Re-Shape Their Disaster Recovery and ...

- Announced today the availability of the final whitepaper in its five-part series, "Rise of the Remote Workforce: Don't Forget About Business Continuity and Disaster Recovery
- Xamin's latest whitepaper offers guidance on necessary components of DR/BC testing and planning, assesses the impact of the pandemic and evaluates potential scenarios to help financial institutions plan for the future

Cybersecurity Update

- HIPAA & Cybersecurity Update - Walmart was sued for allegedly violating California's new data breach law, in regards to lack of proper security with a large amount of customers have their info exposed
- Walmart notified an unknown number of pharmacy customers that their PHI was exposed after several of its California stores were looted by rioters
- Garmin, headquartered in Olathe, KS, announced it was hit by ransomware, which may expose info of customers of its smartwatches and wearables
- ForgeRock 2020 Consumer Identity Breach Report:
    - healthcare accounts for 51% of data breaches in 2020
    - cost the healthcare industry nearly $18 billion
    - each breached record costing about $429
    - second most breached vertical proved to be banking/insurance/financial at 12%.
- Malwarebytes Security published report on malware:
    - AveMaria is remote access Trojan available for purchase on Dark Web for
    - $23/month
    - NetWiredRC malware is used by Iranian sponsored hackers
    - LokiBot uses stenography to hide malicious code inside images
    - AZORult is being used in COVID-19 themed attacks
    - Danabot has been used in malicious PowerPoint presentations
- US HealthCenter, headquartered in St. Thiensville, Wisconsin, notified an unknown number of patients that their PHI may have been exposed after email phishing attack

- Carbon Black Security reports that the Dark Web now has sites selling tax information of people in the U.S., charging anywhere from $50 to $10,000 for content lists
- Positive Technologies reports that 34% of all cyberattacks are ransomware driven during last 90 days
- VPNMentor reported that a group of free VPN apps exposed the private data of millions of users, after more than a terabyte of info was left open on the Internet.
- Tencent is reporting that hackers have created “BadPower” malware, that can infect the firmware of fast chargers (used by owners of laptops, smartphones, etc.) and cause them to overheat, melt components and even set devices on fire.
- Skybox Security report claims a 73% increase in new types of file-encryption malware/ransomware
- Diebold Nixdorf is warning users of its ATM machines that criminals are stealing money by connecting a black box to a USB port hidden behind the front of the machine.
- Federal judge approved a $117.5 million deal to resolve a lawsuit filed against Yahoo Corp. over a data breach that exposed info on 194 million users
    - The law firm who was class counsel received $23 million for their efforts
- U.S. officials ordered the Chinese government to close a consulate office in Houston, TX claiming that it had people inside stealing intellectual property from unnamed companies and organizations in the U.S.
- Li Xiaoyu and Dong Jiazhi of China were both accused by US Department of Justice of working with Chinese government to hacking into organizations worldwide to steal COVID-19 vaccine information
- Joshua Polloso Epifaniou was extradited from the country of Cyprus to the U.S. to face charges of implementing ransomware attacks on organizations in Arizona and Georgia
- Montana Veterans Affairs Health Care System, headquartered in Fort Harrison, MT notified 1,501 patients that their PHI was exposed after malware attack.
- Lorien Health Services, headquartered in Ellicott City, MD, notified 47,754 patients that their PHI was exposed after ransomware attack.
- Smartwatch and wearables maker Garmin, headquartered in Olathe, Kansas, has shut
- down several of its services on July 23 to deal with a ransomware attack that has encrypted its internal network and some production systems.
- First American Financial Corp., headquartered in Santa Ana, CA, is being charged by the New York State Department of Financial Services regarding a breach that exposed

885 million records.

- Metropolitan Community Health Services/Agape Health Services of Washington, NC, has agreed to pay $25,000 to feds to settle HIPAA fines regarding breach of 1,263 patients' PHI
- CSO (chief security officer) magazine published article about threat of hackers using RDP (MS Windows remote desktop protocol) to hack into systems
    - Hijack attempts involve attacker "resuming" disconnected RDP session
    - Hacker can get into device or system without having to steal the user's credentials

- Skybox Security published report on discovered security vulnerabilities:
    - First half of 2020 say a 34% increase in security vulnerability reports
    - Expected to reach 20,000 published vulnerabilities by end of 2020
    - (this includes vulnerabilities found in printers and MFPs)
- CaptainU, an online high school recruitment data, headquartered in Denver, CO, announced that its database has inadvertently exposed the info on nearly 1 million students across the U.S.
- University of Utah Health in Salt Lake City reported third reported email hack of the system this year affected the information of 10,000 patients' PHI
- Gulf Coast Cath Lab of Port Arthur, TX, notified an unknown number of patients that their PHI was exposed after email phishing attack
- Wall Street Journal published report:
    - 80% now view ransomware as a high risk
    - Less than 2/3's of companies have a cybersecurity program
    - 72% have identified critical data assets
    - 45% of smaller companies do not test for email phishing attacks
    - 90% of attacks start with email phishing or social media attack
    - Ransomware causes an average of 121 days of downtime
    - Average ransomware payment in 2020 is $250,000
    - Cost of cyber attack averages $8500 per hour
- The Cooke County Sheriff's Office in Texas notified an unknown number of citizens and employees that their info may have been exposed after data breach
- GreatHorn published results of survey that shows 36% of respondents say they are seeing email threats coming into their inboxes every day

- Barracuda and UC Berkeley published study which found that just over a third of hacked corporate email accounts sustained attacks for more than a week, during which time attackers would monitor how the organization did business so that they could launch subsequent phishing attacks.
- CouchSurfing, an online service that lets users find free lodgings, is investigating a security breach after hackers began selling the details of 17 million users on Telegram channels and hacking forums.
- Ruhr University Bochum of Germany research shows that 15 out of 28 desktop PDF viewer applications are vulnerable to a new attack that lets malicious threat actors modify the content of digitally signed PDF documents.
- The National Cyber Security Centre of England research shows that more than 70% of sports institutions worldwide have been the victim of some kind of attempted cyberattack or hacking incident over the past 12 months.
- Cisco published results of security survey:
    - 77% use over 25 disparate security tools
    - 79% say it is challenging to orchestrate security alerts
    - 69% say 2 or 3 people are involved in a security incident