

# VantagePoint

## E-NEWSLETTER



MONTHLY UPDATES FROM AGVANTAGE SOFTWARE - YOUR PARTNER IN AGRIBUSINESS

October 2021

### INSIDE THIS ISSUE

- 1 Cyber Security
- 4 Upcoming Events
- 4 AgVantage & Windows 11
- 5 Update on New Software Releases
- 6 AgVantage Holiday Schedule



### Cyber Security

By Derek Swanson, Ursa Farmers Cooperative -  
IT Administrator - [dswanson@ursacoop.com](mailto:dswanson@ursacoop.com)

Michelle sent out an excellent e-mail communication on Thursday, September 23<sup>rd</sup> about cyber attacks on ag-business. This email served several important purposes and relayed a timely and re-assuring message. October also happens to be Cyber Security Awareness Month, so I'm very pleased and honored to provide the inaugural guest article this month.

Digressing back to Michelle's e-mail, it got me thinking about our ag co-op IT peer networking group as currently coordinated by Jon Fifer at Posey County Co-op. Since being established – *thanks to Michelle's wise push at an AgVantage National Conference a few years ago* – we've put our heads together on a few big-ticket items like end-user security awareness training and phishing simulations, benefitting from a large group discount on the ever-impressive KnowBe4.com platform. Now, I don't want to make this article all about specific vendor recommendations, but if your company isn't already conducting security awareness training and simulated phishing exercises, that's one name to get that ball started. I can't emphasize this enough: it's not optional, regardless of company size. This is some of the most wisely-spent dollars any company can make since it helps mitigate one of the top initial access vectors for ransomware and other cyber attacks: phishing and email-based malware infections. If you work in IT for your company – including part-time or as an additional job role – and would be interested in joining our peer group or just want to pose a question or solicit for help on something, please let Ben Johnson at AgVantage know and he'll assist in getting you connected with us.

Another initial access vector that was dropping and then actually shot back up due to COVID and remote work is internet-facing RDP (Remote Desktop Protocol). If your company is not able to eliminate internet-facing RDP in the near future, at a

**"I can't emphasize this enough: it's not optional, regardless of company size."**

*(continued on page 2)*

very minimum, it needs to be strongly hardened<sup>1</sup>: enable network-level authentication, implementing a multi-factor authentication solution, using access controls to limit the range of acceptable remote IP addresses, very strong passwords, and so on. Ideally, internet-facing RDP needs to be done away with, so I recommend formulating a plan to implement this over time, whether it's only allowing a VPN connection into the network before reaching an RDP broker or endpoint, or going with a 3<sup>rd</sup> party solution that creates outbound connections to the provider's servers and then to your remote devices rather than punching holes in an inbound firewall. Let me put it this way: HACKERS. LOVE. RDP! It's abused internally as well for lateral movement, so hardening is still necessary.

Beyond that, my recommendation for establishing a proper security posture (read: actually protecting your organization rather than just relying on hope and then having to play the ignorance card later) means having good cyber hygiene<sup>2</sup>, which is a more recent umbrella term that basically describes everything that an organization *should* be doing just to establish a reasonably-secure baseline, doing away with unnecessary risks and the things that introduce the most risk. It will certainly take challenging the status quo. It will require some consulting (tip: cdw.com, connection.com, and other resellers and MSP's tend to offer free security assessments, consulting, and solutions services – you don't pay until investing in the product or service, which allows small orgs to tap into great technical and architecting expertise), planning, vigilance to endure the pushback of initial user grumpiness over changes, and determination to come out from the tough times of the changes but crossing a finish line that upper leadership and your membership can be proud of – a more secure and resilient cooperative! Having said that, most basic cyber hygiene items are honestly low-hanging fruit, and that's why I'm writing this article.

**“...actually protecting your organization rather than just relying on hope and then having to play the ignorance card later...”**

As I go on, I can think of pages and pages of crucial advice to give and information to share on what I've discovered over the years; things to save you the legwork, the precious labor and capital resources, and those things that later, one ponders “why hadn't someone shared this with me already?” Nevertheless, I'm going to cut straight to some final thoughts and key resources to help bolster your security program:

- FREE external vulnerability scanning and internal penetration testing from the experts at DHS' CISA via their Cyber Hygiene Services: <https://www.cisa.gov/cyber-hygiene-services> – just send an email to [vulnerability\\_info@cisa.dhs.gov](mailto:vulnerability_info@cisa.dhs.gov) with the subject line “Requesting Cyber Hygiene Services” to get started.
- Stepping back and basically starting from scratch for small and medium-sized organizations, get realistic, actionable, and bite-size pieces to start putting together your cyber building blocks with CISA Essentials: <https://www.cisa.gov/cyber-essentials>
- Free external open-source scanning of internet-facing resources at Shodan: <https://www.shodan.io/> Check out common ports and services that are running just by entering your public IP addresses. Don't worry about leaking that information as Shodan is a perpetual web-crawling engine like Google, Bing, etc., so anything that's accessible to the internet for more than a few days will be on there, **regardless of whether you know it or not (but better that you know!)**

*(continued on page 3)*

<sup>1</sup>Microsoft RDP Security Guidance: <https://www.microsoft.com/security/blog/2020/04/16/security-guidance-remote-desktop-adoption/?...> (visible URL shortened)

<sup>2</sup>SentinelOne article on Top 10 Basic Cyber Hygiene Tips: <https://www.sentinelone.com/blog/practice-these-10-basic-cyber-hygiene-tips-for-risk-mitigation/>

- Probably the best source for free IT and security policy templates, SANS: <https://www.sans.org/>
- Read Bloomberg's article on NEW Cooperative's \$5.9m ransomware attack if you haven't already: <https://www.bloomberg.com/news/articles/2021-09-20/iowa-based-grain-cooperative-hit-with-ransomware-attack>. What makes this even scarier is that the threat actors don't agree with President Biden's criteria on critical sector organizations, namely that it's safer to target smaller organizations as it doesn't illicit the same national response and outrage.
- Get clear and actionable configuration guidance on security-bolstering controls for most major systems and software in your IT environment, such as Microsoft Windows 10 and Windows Server (GPO policies), common Linux enterprise distros, web browsers, Microsoft Office, and so on: <https://www.cisecurity.org/cis-benchmarks/>. CliftonLarsonAllen's cyber incident response chief and I recommended this in their cybersecurity class at the AgVantage 2021 National Conference. Use CIS-CAT Lite (free) to assess your actual effective policies on computers against the benchmark profiles, which is limited to just Windows and Google Chrome assessments, or upgrade to their premium plan to use CIS-CAT Pro to assess against any software's benchmark profiles.
- For awareness: your data isn't backed up in Microsoft Office 365. I know this comes as a surprise to many, but *cloud* doesn't automatically mean backed-up data – it just means the services are available on the internet and usually in big data centers. Check with your existing backup provider if they offer what's known as cloud-to-cloud backup or acquire such backup capabilities from another, e.g. Barracuda. Also, consider a long-term strategy of migrating toward immutable backups as these can't be destroyed by ransomware.
- Just released! Free 60-day no-cost ransomware risk assessment & remediation service by Qualys: <https://www.qualys.com/forms/ransomware/>

**“...the importance of having a cyber incident response plan.”**

The final topic that I want to close out on is the importance of having a cyber incident response plan. It doesn't need to be highly technical; it's about who's responsible for what, who will be contacted about what, and what communication channels will be used because this should be the assumption: your network is completely down, so you don't have internet access at work or even access to any data on your computers on company premises. Have a contact list with names, positions, cell phone numbers, and email addresses in the cyber IR plan. Print some copies of the plan and distribute to key personnel. As for all IT policies, review annually and update as necessary. CrowdStrike has some great information on CIR planning, including references to some free templates: <https://www.crowdstrike.com/cybersecurity-101/incident-response/>.

In ending, thank you to Michelle, Lisa, Ben, and Elise for your time and support on bringing the new guest article feature to fruition. Take care everyone and God bless!



Providing services beyond the bin



## Reminders for Upcoming Events

By Lisa Sick, VP Marketing & Conferences - [lisas@agvantage.com](mailto:lisas@agvantage.com)

**AgVantage 2022 Executive Conference is February 10-11, 2022 at the Hotel Del Coronado in San Diego, CA.**

This event brings top agribusiness leaders together in a unique way, to share their experiences, successes, and things they've learned in an engaging way. In addition, the AgVantage team will weave into this event the use of the technologies and tools available at your fingertips to help manage your business.

Visit our website at <https://www.agvantage.com/executive> for registration and hotel reservations.



**AgVantage 2021 Pacific Northwest Regional Conference is November 10-11, 2021 at "The Lodge in Columbia Point - Richland WA"**

We hope all of our attendees enjoy our first regional conference starting up again!



## Microsoft Windows 11 and AgVantage Software

By Ben Johnson, Information Technology Services - [benj@agvantage.com](mailto:benj@agvantage.com)

You may have noticed that Microsoft released a new operating system recently and we're excited to see what Windows 11 will offer in the future! For now, AgVantage Software **cautions you to not** do the free update to Windows 11 on your existing computers or purchase your new ones with the Windows 11 Operating System.

We're in the process of testing our software to ensure full functionality with Windows 11. That software includes AgVantagePC GUI (encompassing Point-of-Sale, Grain Scale, and other packages), AgVantagePC Energy (the laptop-in-a-truck software), AgVantagePC ETA (our time tracking software), and IBM's Access Client Solutions. So far, it's looking promising but we're recommending caution when adopting Microsoft's newest operating system.

About Microsoft operating systems, please be aware that Microsoft has ended extended support for both Windows XP and Windows 7. Neither of these operating systems is receiving security updates from Microsoft or from most third-party software companies. AgVantage Software has fully stopped supporting Windows XP at this time. If you're still running Windows XP, we **strongly urge you to upgrade** to a newer operating system or a new computer.

Currently our AgVantagePC products are compatible with Windows 7, but the time is approaching for support to end there as well. Again, we strongly recommend upgrading your operating system or computer to a newer version.

As always, if you have any questions on this please contact us at (877) 282-6353 or via [support@agvantage.com](mailto:support@agvantage.com).



## Update on New Software Releases

By Dave Hammond, VP Programming - [daveh@agvantage.com](mailto:daveh@agvantage.com)

AgVantage strives to meet your agribusiness needs by updating our software platforms on a regular basis. The following is a list of the various AgVantage software platforms and the many new software releases.

### Agronomy Edge

- Remove Seed from Plan reports and screen (492324)
- Add Blending PPA/GA, add show all items check box (500439)
- Show Cost per acre GA/TPF on Products screen (503595)
- Ability to remove individual line items from an activity (512055)
- Fixed Razor tracking issues (541363)

### Accounts Payable Edge

- Trades maintenance needs a few fields increased (525345)
- Invoice Entry - Do not allow comments in lot number field (538788)

### Accounts Receivable

- Do not print Inactive Operators on Restricted Pesticide Report (537383)

### Accounts Receivable Edge

- Move Balance from One Term to Another-Summary (489206)
- Move Balance from one Term to Another-Detail (489209)
- Ability to copy an item to create a new item (511630)

### CRM Edge

- 2021 added for Proof of Yield Year (537941)

### Electronic Documents

- Email list updates after deleting an email (542648)

### Energy

- Tank setting for ACH-add pay type to load for tank file (453869)
- Move tank- 'N' to move History will mark record 'I' and date (491021)
- Ohio taxes -no room in file for -retail dealer-- 5AD code (500411)

### Energy Dispatch Map

- On excel export ask all or only selected columns (503786)
- Add driver#, schedule date and seq# to the hover (505980)
- Dispatching authorities for Drivers (510668)
- Add monitor Y to the dispatching grid (516364)  
- V8.1 Only
- Filter by closed date (518466)
- Load the phone numbers to the LP calls file when creating a call (519045)
- Add loc for price item price out of the master, validate if inactive (520973)
- Add the refill stations to the dispatch map (527505)

### Energy Edge

- CDD #1 - Add an actual tank size (478010) - V8.1 Only
- Dispatch tank map, allow filter by Fuel use (500796)  
- V8.1 Only
- Add tank auditing to Tank Portal to track field changes (509441)
- Add site addr2 to lpcall (526247)
- Add energy comment file (527376)
- Add serial number to the portal tank display screen (530118)
- Enhancement request - Edge Energy Customer Portal (531117)

*(continued on page 6)*

## Feed Edge

Inventory Validation at order creation (376282)  
 On the ration tab add a pricing button (464606)  
 Consultant fee on Cost Plus screen (511060)

## Grain

By Group no longer gives Invalid error msg in Priced Not Paid Report (528052)

## Grain Scale PC

Custom Message Board - Show 0 on Tare until weight is set (535141)

## Interfaces

Displaying trucks on Map can't tell a refined from a propane truck (505976)  
 Add comments, instructions and memo lines to shipto export (538119)  
 Raven interface change for managing multiple API keys (542546)

## Inventory Edge

Add menu option close inventory months (511842)  
 Add item/loc name to inv qty excel download (515823)

## Invoicing Edge

WO come off Contract (485170)  
 Items from multiple locations on one invoice (514996)  
 Add Location to the GL Number entry option (538032)

## Payroll

Adjust Wording on Assign Emp Number Settings (537713)

## Payroll Edge

Employee Maintenance/Portal (453369) - V8.1 Only

## RFID

Add the site and tank to the export file (513533)

## Security

Add NETS command to AGVSEC in green screen (535317)

## Seed Edge

FPOS- implementation and interface (460473)  
 Show Error Descriptions when orders error from Winfield (499716)  
 Create program to move items to new seed year (499782)  
 Page Numbers on Warehouse Report (532486)  
 Increase Manufacturer Order Sequence to 14 (540936)

### AgVantage Software Holiday Schedule

We will be closed or have reduced hours on the following dates to allow our employees to enjoy the holidays with their families.

Thanksgiving	Thursday, 11/25	Closed
Day after Thanksgiving	Friday, 11/26	Open 8-3 (CST)
Christmas Eve	Friday, 12/24	Closed
New Year's Eve	Friday, 12/31	Closed