Cyber Security in Agriculture: What You Need to Know

Description:
How safe is your information? How do threat actors get into your company and what do you do if it happens? Hear from the experts about the current state of affairs and how you should protect yourself and mitigate risk.

Speaker:

- Andrew Rose, Senior Advisor at F3Tech
- Brian Dysktra, CEO - Atlantic Data Forensics, Inc.
- Bill Danker, Principal Industry Consultant - AgTech SAS

Vonnie Estes, PMA:
Welcome to PMA Takes on Tech. The podcast that explores the problems, solutions, people, and ideas that are shaping the future of the produce industry. I'm your host, Vonnie Estes vice president of technology for the Produce Marketing Association. And I've spent years in the AgTech sector. So I can attest, it's hard to navigate this ever-changing world in developing and adopting new solutions to industry problems. Thanks for joining us and for allowing us to serve as your guide to the new world of produce and technology. My goal of the podcast is to outline a problem in the produce industry and then discuss several possible solutions that can be deployed today.

Vonnie Estes, PMA:
This episode of PMA Takes on Tech is sponsored by CropTrak. CropTrak enables food and beverage companies to improve their supply chain management from contracts to settlements, one trusted source of secure data at your fingertips. To track what matters go to croptrack.com/PMA. Hello, today, we're going to talk about cybersecurity and agriculture. Cybersecurity is a very important topic to our industry and to the food supply system. I have three speakers with slightly different takes on the problem and solutions. First we will hear from Andrew Rose. Who's an expert in the topic and is starting a Cyberag organization. Andrew gives us some broad information on what is happening now around cybersecurity. Then we will hear a deeper dive for action from Brian Dykstra, CEO of Atlantic Data Forensics. Followed by Bill Danker, a principal industry consultant from SAS with a view on Ag. This is one of those new to me topics that seems to be what everyone is talking about now.

Vonnie Estes, PMA:
But of course it has been around for a long time and we have been warned to take precautions. What is bringing it to the forefront in the food supply chain

right now is that the Ag industry is particularly vulnerable because we haven't been paying as much attention. The Ag industry has recently adopted a lot of new technology into our operations without the necessary security protocols. Every company is now a technology company, and we need to protect ourselves as such. Let's jump into the conversation with Andrew, where he's talking about the advantages of starting the Cyberag organization in the Maryland area.

Andrew Rose, Cyberag:
If you think about cybersecurity nationally, we've got all of the big agencies in D.C., the NSA, the CIA, and a bunch of others who you probably have never heard about. And as employees work in those agencies, oftentimes will spin out and start government contracting organizations and then organizations that serve the private industry. So we've got a real good, critical mass of these types of companies, individuals, thought leaders, and what have you. So it was almost a blessing to be able to stand this organization up in that area. And I've always stayed involved the cybersecurity. I've spent the last six years in agricultural finance, and it was funny. One of the first things I did when I came to the bank was I put on a tabletop exercise, simulating an insider attack on our systems from a cybersecurity angle.

Andrew Rose, Cyberag:
I just recognize that there wasn't a whole lot of awareness in the bank. We felt that our defenses were good that we weren't necessarily a target. And what have you. And it was a very instructive event. I won't go into too many of the findings of it, but one of the outcomes was it helps us develop muscle memory. So if something like this does happen in the future, at least we're not relying upon documents that may have been created by somebody else that we pull off the shelf and flip the page three and say, "How do we contact folks?" We actually put these things into play into motion. Fast forward to late 2019. And I was invited to attend a private briefing from one of the head intelligence people on some of the threats that China posed for intellectual property theft to a multitude of industries.

Andrew Rose, Cyberag:
And after that briefing, I spoke to the authority there. And I said, "I'm in the agricultural sector, is this something we should be paying attention to?" And his face went ashen and he said, "Oh my gosh." He goes, "The agricultural sector itself is so at risk right now, we need to get the message out there." And almost simultaneously, I was recognizing at least in the State of Maryland, that agriculture wasn't getting the attention from the economic development people. That cybersecurity was.

Andrew Rose, Cyberag:
In a nutshell, if you put the word cyber in the title of your company, people throw money at you, and they don't really understand what you do. You have

agriculture farming in your title, and they tend to relegate you to the children's table. And so I approached a good friend of mine, Mike Thielke, who runs an Ag incubator called F3 Tech and said, "Mike, we're going to put on a symposium about cybersecurity in agriculture." He said, "Andrew, what does that mean?" And I said, "Mike, I don't know what it means, but we're going to do it anyway. And we're going to find out what comes of this."

Andrew Rose, Cyberag:
So I invited the intelligence community to come in and speak. And I reached out to the USDA and the USDA brought their chief information security officer out, and we did a full symposium, and it opened a lot of eyes. It really got the ball rolling and dumb luck-

Vonnie Estes, PMA:
And this is before there had been attacks in Ag, right?

Andrew Rose, Cyberag:
Vonnie, you're reading my mind. I'm so dumb luck. We put the symposium on one week before the SolarWinds breach hit the news.

Vonnie Estes, PMA:
Oh, gosh.

Andrew Rose, Cyberag:
We are very smart. We probably looked a lot smarter than we actually are, but timing being everything was fortuitous. There was a lot of attention given to us. We recognized immediately. We had to do a follow-up symposium. Some of our friends, I'm in the Delmarva area and we've got billions of dollars in poultry and broilers. And one of the large integrators is Perdue Farms. And they were seeings many or some of their contract growers being hit by threat actors in the cyber sector. And it was having a significant impact on those producers' businesses. So we approached the FBI and we did... And it says, this is widely available and I'm sure we can share links later, a video that describes some of the top attacks that are hitting growers right now, and the FBI then saying, "Here's the mitigation, after the airbags had gone off, here's what you do. And here's why this matters. And here's how we will then perform."

Andrew Rose, Cyberag:
And Vonnie, again, you hit the nail on the head. It seems that this is really an escalating area of concern in the agricultural community. So as of August 1st, I've decided to leave Farm Credit and full-time run the Cybersecurity Agriculture National Center, and we're standing this up right now. It was an initiative. And now it's a thing, and I'm very excited about this. And so the timeliness of this conversation is just fantastic. And I'm sure your listeners are going to be eager to hear what we have to share today.

Vonnie Estes, PMA:
Yeah, I think when I contacted you through Seana Day, a mutual friend of ours and things were just going crazy for you that suddenly you're the expert, and everyone wants to know about this, and you're just starting to stand up this new organization. So it is a topic that's suddenly everybody wants to know about. So if you can walk us through why is agriculture a target for threat actors? Like why is Ag important?

Andrew Rose, Cyberag:
As important as we know agriculture is when you look at the entire landscape across the country, agriculture typically falls to the bottom of a lot of lists. It is considered part of the critical infrastructure, one of 16 critical infrastructure categories, but we tend not to get any attention both from the cybersecurity experts, as well as the threat actors and those days have ended. I think that there is a sense of complacency sometime the cultural sector, because we haven't been hit as hard or as frequently, but now with the sophistication of the threat actors, they're looking for any target out there. And there's a dawning realization amongst our adversaries or those that have a financial interest in attacking us that there's a lot of leverage in food.

Andrew Rose, Cyberag:
You take food out of the equation and people get very hungry, very fast, and it tends to healthcare is another one. I mean, you're seeing it in the hospitals. If you take a hospital offline, they're more apt to pay whatever ransom to is to get back online quickly. Very similar concept with food and take that off the table, so to speak. But going back to your question, agriculture presents a lot of soft targets for the threat actors. Defenses are fairly porous at times. And if you look at the backend technology that a lot of the producers through agribusinesses are using, they're not always state-of-the-art, they'd never had to be. But this is a new day has dawned upon us in this aspect.

Vonnie Estes, PMA:
So what are the current threats and what do you think the future threats are?

Andrew Rose, Cyberag:
That's another good question. This is an important one as well. The current threat as of the latest data breach research that I've seen are financial in nature. There is so much money to be made by these criminal gangs out there holding people's information ransom, holding their supply chains ransom. People are paying that money. And I think we need to back up a little bit, talk about ransomware itself. Everyone's probably heard of ransomware, but if you think about it philosophically, if you put yourself in the shoes of a bad guy, and let's say, you're just starting out, let's say you get into a company and steal that information. The amount of money you will get for that information on the black market degrades from the amount of time that you have it.

Andrew Rose, Cyberag:
So somebody recognize that their credit card has been stolen. They'll stop that credit card. Their personal identification information just stolen they'll put credit watches and things like that. So you need to sell it quickly. Now, if you're a buyer of this black market information, you want it to be fresh, but you also want to buy it from someone you trust, which sounds bizarre. So the large ransomware gangs are the ones that people trust to buy this information from. So the smaller ones typically will sell that information upstream to the larger resellers, and they take a cut of that. They also will sometimes get into a system. And typically they're in your system for four months, is the average amount of times they move around laterally. They find out when the most vulnerable time to execute the lockdown to encryption of your data is, and they sell all those keys upstream to large gangs.

Andrew Rose, Cyberag:
And another thing to keep in mind for your listeners is when a ransomware team gets into your system, one of the first things they do is they try to disable your backups because they don't want you to have any kind of mechanism to recover that data or take them out of that financial equation. Another one that we're seeing, it's not quite as prevalent as their ransomware on the financial side are competitors, and a competitor could be another business. There could be some sort of trade secret that another business would benefit from knowing about from what you have. It could be another nation state, China doesn't play by the same rules we do. They're a country, they have their own ethos and how they operate. And if we're willing to have all of our information out there for the taking, they're just going to take it, why would they spend all that money doing research if they can just get that right now, out there from one of our competitors. And we can go in some case studies and a few minutes about that?

Andrew Rose, Cyberag:
And the other one that that gets headlines. And I haven't really done the percentage of these are the hacktivists. Those are the people that might not appreciate animal, livestock raising or processing and insider threats. There could be some folks out there that for whatever reason are dissatisfied with their employer, and they're willing to either through malice or for financial gain turn some of that information over, but far and away the greatest one is ransomware. That's the easy one, the easy target right now. Now you mentioned the future. We talk about the financial gain of some of these threat actors.

Andrew Rose, Cyberag:
In my humble opinion, the future are going to be adversarial nation states. It's going to be very apparent that if they want to slow us down or cripple us in some way, going after our food supply is target that I would imagine would be fairly high on their list. And it doesn't always have to be an adversarial nation

state, either. It could be a friendly nation state. There were other countries that could benefit from a dip in our agriculture production in a given year that would then increase the amount of money they would make off of their exports or agriculture production. And one area that the FBI is really concerned about is something called deepfakes. And you may have heard about people whose images and voices are now being manipulated through computers, and it's becoming more and more difficult to distinguish those voices or images from a real person.

Andrew Rose, Cyberag:
This is an emerging threat and will only become more and more sophisticated as we go on. So it could be that you get a phone call from the CEO saying, "Hey, we've decided to change our relationships. Please change the wire information to here and send all reminders to this bank account instead." And you will converse with this person. They will sound and use the same idioms that your CEO may use. And you don't think twice about that. Or it could be you and we can get into this later, you have an internal mechanism where no bank information can be changed or shared without the CEO's verbal approval. And you call the CEO up. And that CEO says, "Yes, thank you for calling me. And yes, execute that bank transfer the way I've told you to do." And it was a deepfake all along.

Vonnie Estes, PMA:
Oh, my gosh.

Andrew Rose, Cyberag:
So this it's future, but it's near shore future.

Vonnie Estes, PMA:
Yeah. So how are these threat actors getting into agriculture businesses? You mentioned they can go in and sit for four months. How do they even get in?

Andrew Rose, Cyberag:
Right now, as of the 2021 reports that I've read, the number one way is social engineering. So they identify people who might be in charge of finance or your CFO, and they have a long-term campaigns to build a dialogue with these people. And the stuff I'm seeing now is mostly the threat actors are mostly human, but when we start talking about the use of artificial intelligence, they can do a lot more data mining. So I would imagine that if we're not seeing it today, we'll probably see it tomorrow that are human beings utilizing artificial intelligence to gather more data. So they know what kind of sports you like and what kind of food you like. They can build that dialogue and create a friendship with you and rapport. And then I imagine in the not too distant future, those will be completely AI.

Andrew Rose, Cyberag:
You might think you're having a conversation with a human or interacts with

the human, and it's really a bot out there that's been trained to emulate another human being and all that to get inside of your system. And again, I don't want to disparage the Ag system, but we have a lot of unlocked doors. There are a lot of methods for folks to come in. We talk a lot about the information, or I'm sorry, the internet of things. So all your sensors, all your cameras, all those other little nodes that someone can creep in, get into your system and then start moving around laterally.

Vonnie Estes, PMA:
So all these sensors that we're so excited about that are everywhere in the fields and giving all this information back and forth, those can be kind of portals of entry?

Andrew Rose, Cyberag:
They really can be portals of entry, but also portals to exfiltrate certain amounts of data. So right now, data is one of the new currencies in agriculture. And if so, if you're leaking that data to somebody and they're listing or gathering that data, now the value to you for that data decreases, and they have access to that. And going back to financial incentives, if you're a threat actor and you want to get somewhere, the easiest thing to do is open the checkbook. I mean, ask 100 people and one will say, yes, maybe they have financial issues, they're medical related or gambling related, or they're just greedy. It's very easy to buy somebody off. And our adversaries recognize that. One of the associations that I follow quite closely is the Animal Ag Alliance. And they've done a really good job of understanding or identifying the hacktivists and the insider threats and how to mitigate those types of things. So I don't know if your listeners are familiar with that association, but I believe some of their videos or documents are available online for general viewing as well.

Vonnie Estes, PMA:
That's sounds good. We'll have to put that in the notes. What are some other ways that producers and Agribusinesses, how can they protect themselves from this?

Andrew Rose, Cyberag:
Well, I think it all starts with identifying what are your crown jewels? What does that thing that is most essential to your business that would cripple you if that thing was lost or locked away or given to a competitor? Once you've identified that then make concentric rings of security around that. A lot of the stuff is pretty basic blocking and tackling. When that little window pops up to upgrade your Microsoft, click it say yes, always upgrade and patch.

Vonnie Estes, PMA:
Oh, all those updates putting off those?

Andrew Rose, Cyberag:
Oh, men. And they're annoying. I know they're annoying because sometimes they come unexpectedly and your computer goes blue for 20 minutes. When in the middle of an email, they're crucial. And the reason they come in that way is Microsoft, or whoever it is, is identified a threat that somebody is utilizing right now. And they want to protect all the users. Please don't put those off. An example is the Baltimore City school system, I'm from the Baltimore region, put those off because they didn't want to be inconvenienced because they had to send emails out and the entire system got hacked and then locked out by ransomware. It's these things. It sounds very basic, but it's true. Another one is when you do your backups, when you take all that data and whether you do it weekly or biweekly or daily, take it and remove it from the computer and they call that an air gap.

Andrew Rose, Cyberag:
So that makes it a little bit harder for those threat actors to come in there and to travel to that backup in that way. It's a little bit easier to put that in there. We talked about the information of, or I'm sorry, the internet of things. Put some passwords on these devices. A lot of times they come with a factory basic password and people don't think to change that or updated at times, that's always a good idea. There's a term called multi-factor authentication, and you may have seen this where you log into a website and they text you a code. So is two steps in order for you to access that. If you have an opportunity to turn that on, that's an important one and...

Vonnie Estes, PMA:
Those are so annoying though, but you're telling me those are important that we should-

Andrew Rose, Cyberag:
And going forward, they're going to be ubiquitous. We have to, gone are the days when you have a four digit password and think your Hotmail countless was protected.

Vonnie Estes, PMA:
The same password you've used everywhere.

Andrew Rose, Cyberag:
Yeah. It is. I know. And well-

Vonnie Estes, PMA:
Your birthday.

Andrew Rose, Cyberag:
Correct. And that kind of goes to the next one. Is employee training on cyber awareness. There are a lot of organizations out there that provide basic training. Here's what a suspicious spoofing email will look like. Here's when

you want to pause before you click on that link and do that thing, and then maybe send out some rudimentary testing. You put the employees through this, well, let's just send out a fake phishing email and see who clicks on it because that's the person that you probably want to have to go through additional exercises. I love tabletop exercises. I know it takes a lot of staff time to do these. It's a four to six to eight hour session, but you have everyone sit around the table and go through the what if scenarios. Let's just say that everyone comes to work in the morning and all of our computers go black, or what do we do now?

Andrew Rose, Cyberag:
And then kind of walk through these exercises and you start identifying different gaps that you might have there in your crisis plans. I won't go too deep in that because you always discover things and you probably don't want to share those publicly where the holes are. And then last there is cybersecurity insurance and a lot of people think, "Well, I pay the premium so I don't to worry about that." What they don't recognize is cybersecurity insurance. They're becoming more and more reluctant to pay out if you don't have good internal controls, if you're not following these things that you should conversantly, if you do follow these things and you have best practices, and you can demonstrate that sometimes there's a reduction on premium or you get more coverage for your dollars. Hygiene matters a whole lot.

Vonnie Estes, PMA:
Yeah. And I think on the insurance piece, from what I've heard too, is that they may help you financially, but you may have had a huge reputation hit that you can't recover from. If they've gone into your customers and attacked your customers, you've lost in trust there. So insurance doing hygiene upfront is better than insurance, but insurance can help. So what can a producer or a business do if they are attacked? We've heard even in our industry and the produce industry, there've been a couple of ransom attacks where the companies paid the ransom because for all the reasons we know it's just cheaper to go ahead and pay it and move on. But is that the best thing to do? What should people do if they're attached?

Andrew Rose, Cyberag:
That's a great question. I know that we have somewhat of an international audience for this podcast from the United States, there's a website called ic3.gov. They should go there immediately log what has happened. And that website is a portal for all of the law enforcement intelligence community. So that triggers a response number one, but it also logs trend analysis. The law enforcement would love to be able to get ahead of these so that they start seeing a certain sector or a certain methodology being used to go after these companies. They can start getting ahead of that and either pretty warnings out there or starting to anticipate what the next move is.

Andrew Rose, Cyberag:
I'm a huge proponent of bringing the FBI in as soon as possible. And I know something that makes some people nervous when you call the FBI, the FBI is very clear. They are there to impose risk and consequence on the bad guys. They want to make it, they're not there to blame you for doing something that you shouldn't have done clicking on a link or letting somebody in, they're there to find the bad guys and impose consequence upon them. The FBI will also tell you "Don't pay the ransom." And this is one of those push and pull things. Some companies, this is a cost of doing business. If you're colonial pipeline and now there is no more gasoline in the Northeast United States. Yeah. You're probably going to pay that bitcoin ransom and see what happens.

Andrew Rose, Cyberag:
Now, here's where the supposition comes in. I don't know necessarily who took dark side, that ransomware gang offline, I don't know who sees their servers are clawed back some of that bitcoin payment nor do I think the FBI would ever admit to being part of that, but that's the consequence and the risk is now the next threat actors and say, "Ooh, maybe I shouldn't go after the gas pipelines," which their new inception has put that as a public statement. The bad guys said, "We won't go after the critical infrastructure, we won't do this." It's a cat and mouse game.

Andrew Rose, Cyberag:
And then you talked about the ransom payments. That's ultimately it's a business decision to be made. Again, the law enforcement community would rather you not do that. It makes their job more difficult. And also they'll let you know that if you pay that ransom now, you're out there on the dark web bulletin boards as somebody who's stroked a check to get your data back. So now you're more likely to be attacked. But I can see it from a business standpoint too, I'll pay the million dollars, just so my $20 million or a hundred million dollar business can get back online as quickly as possible.

Vonnie Estes, PMA:
Next we will hear from Brian Dykstra, from Atlantic Data Forensics. Brian has been at this for a while. He talks about the easy things we can do to protect ourselves. Here's Brian,

Andrew Rose, Cyberag:
Sure, so I'm Brian Dykstra, I'm CEO of Atlantic Data Forensics, where they call it DFIR providers. So we're a Digital Forensics & Incident Response company, which means that we're the folks that you call when you got ransomware or you had some fraud or business email compromise, or we just handle people's worst days really. And we do it over and over. We do hundreds of incidents every year, thousands over the past 15 years. Got started doing this... Well, I grew up as a farm kid in Oregon joining the military got a FFA chapter president.

Vonnie Estes, PMA:
That's impressive.

Brian Dykstra, Atlantic Data Forensics, Inc.:
Got into military intelligence with the army worked humid and technical intelligence. And of course, when you leave the military, what you do is you go to a defense contractor. It's an easy transition back into the world. Ended up teaching cyber crime at the FBI Academy at Quantico for a few years to the super cops. And that just continued on that career from there. 2003, Kevin Mandy, and I started a little company called Mandy and it turned out okay, it's a multi-billion behemoth now. So this is what I do, now all day every day.

Vonnie Estes, PMA:
So do you work in the food supply chain? Is this an area that you've had some involvement in?

Brian Dykstra, Atlantic Data Forensics, Inc.:
We do, we work both in the food supply side as well as in the grower side, the equipment providers side, because nobody right now is invulnerable from ransomware or these business email compromise attacks that lead to further ACH fraud as is, I mean the threat actors are doing this. They don't really care what your business is. They care less about what you do for a living they're about your bank account. And then since so every business has one, the threats now spread across every industry. So where in the past, we might've been sectored around regulated data industries, healthcare, or finance, or things like this. Now we're dealing with everybody because it they don't discriminate anymore.

Brian Dykstra, Atlantic Data Forensics, Inc.:
It just doesn't matter. And we've seen that in the press recently. It's all different companies and all different industries getting hit. So is that, but for AgTech, and Ag is the larger Ag communities and stuff like this, extra vulnerable just because there hasn't been a lot of attention really paid to this over the last 10 to 15 years. I mean, there's been some discussions here and there and the USDA has got a nice little website in a report of that maybe, but they're not really, there's not a lot of emphasis in the larger agriculture and food community into that sort of thing. And so unfortunately, we're sitting on a lot of tech debt, we've started to bring these technologies into everything we and into the manufacturing process, and packaging and shipping and transportation, you name it without a lot of security oversight into what's been added on there and what happens if something goes wrong.

Vonnie Estes, PMA:
So are there specific things that the food supply chain should be concerned about that are specific to food and Ag?

Brian Dykstra, Atlantic Data Forensics, Inc.:
Yeah, so, I mean, everybody's kind of problem number one is ransomware. Because while it's highly preventable, it doesn't take much to keep ransomware threat actors from getting to your company. Most companies just aren't even aware of what they need to do to prevent that. And it's really simple little things. Securing the perimeter of your network properly. Unfortunately most of the ransomware that we handle, they walk right into the door through unsecured services and things like this that the company's had there for years. We just always did it like that. The hackers will find that and they will make you pay for that. There's still this idea that you can use a user ID and password on the internet and that's good enough.

Brian Dykstra, Atlantic Data Forensics, Inc.:
That's not good enough anymore. That hasn't been good enough for the last few years. You have to use what they call multi-factor or two-factor authentication which we've all seen. I mean, your bank probably makes you do it now, or PayPal makes you do it, and all these other companies make you do it.

Vonnie Estes, PMA:
Its really annoying.

Brian Dykstra, Atlantic Data Forensics, Inc.:
It is maybe, but is it really, I mean, how many times a day do you push a button on your phone anyway? I mean, you've got to put four or five, six characters in just a logging into the darn thing. It's not really that big a deal to go. Yeah, that was me logging into the VPN click.

Vonnie Estes, PMA:
Yeah, I think that's really true.

Brian Dykstra, Atlantic Data Forensics, Inc.:
Is it really annoying or do we just dislike the idea of there's change necessary and the reality is we just don't like change. But that's what gets people into trouble. Because most, again, the ransomware we deal with, the threat actor logs in right through their VPN, because they've stolen a user ID and password there, and then they're inside their network and they go about deploying their ransomware and so on. There's also that prevailing idea out there that's just really old and internet time, which makes it three or four years old. Somehow, John in marketing clicked on a link and that's how we all got ransomware. That hasn't been how we got ransomware in the last three to five years. That's just not real anymore, but unfortunately that's companies tend to put all their emphasis on that sort of idea. So...

Vonnie Estes, PMA:
So how do we get it, how does it get in?

Brian Dykstra, Atlantic Data Forensics, Inc.:
We get it through stolen user IDs and passwords. And they actually log right into our network through our own remote access, through our Citrix, through VPN. I think it's like that that aren't secured app. And then they just go to town and they deploy it from the inside of the network. And then same thing we don't have, most companies have little to no visibility inside their network as to what's going on from server to server to continue. I'm constantly amazed by how many multi-million dollar companies I work with the don't even have antivirus on their computers in there. It might be on their desktops, but somehow their cloud and server environment, they don't have anything running on them and they can't see what's going on. And so they're just easy picking for a ransomware threat actor.

Brian Dykstra, Atlantic Data Forensics, Inc.:
And then unfortunately there's lots of them out there taking advantage of that situation. And realistically, we look at those two factor authentication, control the bad stuff on the edge of your network and put two-factor on things or AV on things. That's not a hard thing to do. I mean, those are all pretty low bar things. And maybe the last thing is just when that pop-up pops up and it says, "Would you like to patch?" Say, yes.

Vonnie Estes, PMA:
Yeah.

Brian Dykstra, Atlantic Data Forensics, Inc.:
Say, yes, Google puts a little thing in the corner and says, restart the update, say, yes. It's free. But we find all the time folks running just the pool, horribly outdated software. And that's the other way that they easily take advantage of us. And the threat actors that are out there right now, it's not super severe, I don't know. Not to say that there aren't nation, state, threat actors out there that are pretty sophisticated. Yeah. They are. They definitely are seen as some exploits by those that are unbelievably complicated, but your average ransomware threat actor, that's going to cause most of us problems they're not sophisticated. They're taking advantage of the really, really simple stuff, which is like you just said, the things I just listed, just the really easy stuff. They're not doing anything complex. They're not particularly skilled. They don't have to be.

Vonnie Estes, PMA:
Yeah, exactly.

Brian Dykstra, Atlantic Data Forensics, Inc.:
To get into most places.

Vonnie Estes, PMA:
So do you work with companies to help prevent attacks or are you mostly response attacks?

Brian Dykstra, Atlantic Data Forensics, Inc.:
I would love to, I really would. And we do get an opportunity to, if I'd have gone out to a big airlines company next week that really focusing on getting ahead of the threat to their operations. But in general people don't because you've got other business priorities and I get it. I only got what I need. You've got other business priorities that are the things you're worried about. The next two customers, you're onboarding things like this. We'll, get to that IT whatever, somewhere down the road. And that's this mistaken idea that whatever your business is that isn't also a technology company.

Vonnie Estes, PMA:
Yeah, that's the point.

Brian Dykstra, Atlantic Data Forensics, Inc.:
We don't have any non technology companies anymore. I mean, I'm sure we do, but they're few and far between most of us, we really rely on that technology nowadays just to make anything happen. And so it deserves that level and importance within the company. So some companies are starting to catch onto that idea, but for the most part, that is just not the case. And unfortunately I end up just getting the call at 3:00 in the morning on a Saturday morning, text I mean and...

Vonnie Estes, PMA:
So what should people do when they are attacked, they should call you at 3:00 in the morning or what should they be doing?

Brian Dykstra, Atlantic Data Forensics, Inc.:
Yeah, that's why we have the 1-800 number for this call us 24/7 real personal answer, the phone and help you out.

Vonnie Estes, PMA:
And they should do that quickly, right?

Brian Dykstra, Atlantic Data Forensics, Inc.:
Yeah, you want to get ahead of it. As much as possible, what should really be doing, you should be planning ahead of it, knowing that you aren't going to do that. You should have some plan for if we do get in trouble, where do I call? And unfortunately, a lot of times folks just don't know, they've never ever thought about what might happen. And so we see some of the... and clients that called their CPA firm. I don't know why, that was your first call. You're like, "Why, why, mm-hmm (affirmative) I'm not sure what that was about, but okay." Or they call their IT company it was probably the ones that got them involved in some of that to begin with. So that's not necessarily a help. And there was just a lot of things going on out there. Other folks call their local police department or try and call the FBI or stuff like this.

Brian Dykstra, Atlantic Data Forensics, Inc.:
They're not going to help you. They're more than happy to take the report, but because it feeds the stats engine, but they they don't send teams of people out to help you get it corrected or tell you what to do or anything like that. So, yeah. So in a lot of cases, you're on your own and it takes just a little bit of prep work. I mean, get with your insurance provider talk to them about cybersecurity insurance and maybe I need to add something on, that's getting much more expensive and harder to get nowadays.

Vonnie Estes, PMA:
I bet.

Brian Dykstra, Atlantic Data Forensics, Inc.:
But again, because of ransomware. But reach out to, or even your existing IT provider, honestly they've probably been coming to you for a while and saying, "Hey"-

Vonnie Estes, PMA:
Now, I want to pay attention to this.

Brian Dykstra, Atlantic Data Forensics, Inc.:
"Talk to you about security ideas you probably need one." No, no, no. Enough of that. They don't need to hear any more of that. But maybe take a listen, go, "Hey, what do you guys got? What are we missing?" Things like that to try and get a little bit ahead of it.

Vonnie Estes, PMA:
And what about the people that just say, "Okay, I'm just going to pay because that's cheaper." Than try to go through all this?

Brian Dykstra, Atlantic Data Forensics, Inc.:
Right. I mean, we look at all of this so we negotiate with ransomware threat actors on a regular basis. And we do pay ransoms on behalf of our clients. But it's only at about 15% or less of the cases that we actually do that. So we take a real close business look at what is our business case for paying this? Why do we pay? Now, if you have a company where look, we have no backups and 100% of our systems are encrypted up and we're just stuck. All right, you're going to need to pay. There's not a lot we can do for you, but if we've got partial backups or some backups, or we can get this system, this necessary for business operations back up and running by reinstalling or reestablishing it or things like that.

Brian Dykstra, Atlantic Data Forensics, Inc.:
Maybe there's not a great business reason for us to pay for a decryptor and things like this. It varies because if you have data stolen, which is a common part of these ransomware events now, you're still going to have to do all that reporting. So if you had even lost HR data, you got to report to state's

attorneys generals. And if you have a regulated data, you're going to have to port the government agencies, you're going to get penalized and all these things. So you're going to do all of that anyway, whether you pay or didn't pay. So that's not really a factor, you're going to do all those things. And if you have customers, you're going to have to do credit monitoring for them. So you're already going to pay all those things.

Brian Dykstra, Atlantic Data Forensics, Inc.:
You're going to deal with all those legal fees and that. So if there's probably not a reason to pay to try and get your data back. And that's the other thing is this idea that you're going to get your data back. You're going to get your data back, but they're also going to keep a copy of it and they're going to sell immediately on the dark net. And then that's just what they do. All your big hacking groups do that. So that idea that you're somehow going to magically give you data back or things like this, and not without a copy going out for sale, because they're very much like organized crime, they're there to make a buck. And there's value in your data. It might not be a lot of value, but some value to somebody and somebody will be willing to buy it. That's just more cash in their pocket for no of a little work.

Vonnie Estes, PMA:
Okay. Well, I think-

Brian Dykstra, Atlantic Data Forensics, Inc.:
I know I have no good news for you.

Vonnie Estes, PMA:
Still so helpful. I know. Well, I'll make sure and put a link to your company in the show notes.

Brian Dykstra, Atlantic Data Forensics, Inc.:
Appreciate that.

Vonnie Estes, PMA:
I think it's just good. Just these conversations just really important for people to hear them and how important and easy some of the mitigation is. So thank you very much. I appreciate your time.

Brian Dykstra, Atlantic Data Forensics, Inc.:
Goodbye. Pleasure. Thank you.

Vonnie Estes, PMA:
Now we will hear from Bill Danker of SAS, Bill's role is to deliver technology solutions to the Ag industry and include cybersecurity in those solutions to keep us safe. Bill Danker, AgTech, SAS: Hi, everybody. This is Bill Danker. I am a principal industry consultant with SAS statistical and analytics company here based in Cary, North Carolina. And my responsibilities here are really to

provide support and help in the delivery of analytical solutions for agricultural companies. And that includes the delivery of agricultural systems to help and make decision support and analyzing yield and improving nutrient content, and also looking at cybersecurity of those solutions and how they could potentially whether they need to do to keep themselves safe. In the application, a lot of these applications.

Vonnie Estes, PMA:
So are there specific things that agricultural companies should be concerned about and what are the potential kinds of attacks that you've seen in looking in this area? Bill Danker, AgTech, SAS: Well, there's always the normal they're after your personal information. I call that the baseline. We're all aware of it. Folks use phishing attacks and other types of attacks to try to get your personal information so that they can steal your identity and go with it. From an agricultural perspective. That's always going to be a concern typically for farmers, large farming operations you don't want to get hacked and then have your personal information stolen at the deal with it. I do think in today's world, it's more of the ransomware level. So we've got the recent example of JBS, the beef packing company. The pipeline that got shut down, those are all examples of ransomware attacks. And for those that maybe don't understand what that is, is nefarious groups. They get bots implanted in your systems. Bill Danker, AgTech, SAS: They're able to then put in an encryption layer across all of your data. This goes on for awhile. It doesn't happen overnight. They're in, this thing gets, and then they wait for the opportune time when they can shut down your systems basically everything gets encrypted and you can't read it. And then suddenly you can't operate and they'll wait for the right time, like the end of the month or when the dollars are going to come in. That you're most exposed because what they're after is money. All that matters. They're not after stealing ID, they're just after the money. But the exposure it is for us, at least from an agricultural perspective as they can shut down aspects of our agricultural pipeline. And that's a major concern for us as an industry. In terms of what folks should do about it. You can go to all of the standard, make sure that everybody is password protected and you're doing all of the baseline security protocols in place. Bill Danker, AgTech, SAS: But what I would recommend to a lot of folks is you do a tabletop test of your systems. So if you've got it's typically for a ransomware perspective, plan it out, pretend like you got an attack, take a look at your backups. How often are your backups being run? Can I restore from those backups and be running within a day or two? The ransomware attacks, if they're there long enough, they'll make it into your backups. So even going to that, isn't going to help you. And have you thought through the implications of all that? So I know a little bit long there, Vonnie, but that's where I think the biggest threats are at today.

Vonnie Estes, PMA:
And how do they get in, how do they even get a foothold in and start getting inside your programs? Bill Danker, AgTech, SAS: It's malware that sneaks it

away in and there'll be getting very, very good at it. We held a forum last week on cybersecurity. This is the one that I didn't even know about. So in today's world, you go into a restaurant and you scan the barcode, but you can get the menu up. And then you can look at the menu for the restaurant, depending upon the security protocols that, that restaurant chain has implemented. It's possible to get malware embedded in that barcode. When you scanned it. It's now on your phone. It's now creeping through your phone, your systems. I don't want to scare everybody with that one, but the potential is out there, any kind of those phishing attacks you get the text messages that says, "Hey, it looks like Wells Fargo. You need to respond to this." Any of those layers where you accept it, and then you've got something coming back onto your phone or onto your device. That's how they get in. And you won't know it. It's a bot that then takes off and it starts replicating itself throughout your systems.

Vonnie Estes, PMA:
And those should the backups that you do. I mean, are you protected by if you keep your updates up to date or is there any way to protect yourself there? Bill Danker, AgTech, SAS: You definitely want to have the disaster recovery protocols in place. Again, for companies where you're taking the backups, either weekly or monthly, every six months, you've stored some of them away. It depends on how much you're changing things. Again, as you're changing applications that you're running with, that might impact how you might recover it because you might have to go back six months to that backup and then restore and run from that. So what's the implications if you have to do that? You can have backups to go back one, two years, and then that you're going to be fairly safe, the issue. And this is why I recommend the tabletop exercise. Well, what if we had to go back a year and restore everything? What are the implications to the business? Bill Danker, AgTech, SAS: And can I effectively do that and be back up and running? So I'm not having to pay the ransom. And for a lot of companies, they just pay the ransom. There's a lot of ransomware attacks. You and I will never hear about. Because they hit at the right time, the finance guy that looks at the dollars and go, "We're going to lose this much money. So they're going to cost me this much to pay him. We keep it under the covers. We pay him and we go on."

Vonnie Estes, PMA:
So when you do pay him, do you get your data back? And are you hold-in? Or what happens if you do go ahead and pay the ransom? Bill Danker, AgTech, SAS: They basically release that encryption, that was spread through your systems and all your data becomes readable again. You're basically, you're up and running in a matter of a few minutes.

Vonnie Estes, PMA:
But then did they sell your data? I mean, do you see? Bill Danker, AgTech, SAS: They could. That is the other issue. When we talk about this thereafter money. And you hit on the second one that's also very important. Any

intellectual capital that you've developed as a company, if they've gotten in chances are they've pulled that off and they could leverage it to get money in other ways. The other one I thought was interesting that I learned about last week was what if you know that you've penetrated a company and you then announce it, that they're going to get shut down via the dark web, whatever. I can now have partners that can short that stock. And then when it actually hits the press, this company is shut down. Their stock takes a dive while they tried to recover from it, pay it off, they make money both ways. They make money on the ransom that they clear it, and they also make money if they're getting really that... I mean, the challenges are many.

Vonnie Estes, PMA:
Yes. So what should a company do if you come in in the morning and you try to start your computer up and you've been attacked, what are the different options of what company should do? Bill Danker, AgTech, SAS: In most companies there's usually a help desk where you call somebody right away and say, "Hey, I've experienced this." At a previous company, I won't say which one. I got a strange email. It looked like a phishing email. So what I did was pick up the phone and call the security office right away and say, "Hey, I've got this." And there was a couple of times where like, "Oh, bill, can you forward that to me or send me a screenshot of it so we can look at it." Bill Danker, AgTech, SAS: And then they can shut it down on their end in terms of understanding the IP, where it's emanating from and get it shut down that way. From a SAS perspective, I'll be talking about what we do, we've got algorithms in place that can monitor internally what's going on across a lot of your systems. And we can flag when something out of the ordinary starts to transpire, may not be an attack, it might be an attack, but it raises the awareness of something going on in the data. And you can then highlight your security folks who can take a look at it quickly and understand if they are under attack and respond to it much more quickly.

Vonnie Estes, PMA:
Great. Okay. I think that's given people some things to keep them awake at night. So thanks for that. Bill Danker, AgTech, SAS: Always be vigilant. It's always a matter of being vigilant and being aware of the different types of attack. And again, I can't stress enough doing the tabletop exercises. A lot of companies, they've got a disaster recovery plan. They've got a plan in place, run those through, practice them daily. It'll really help you be better prepared.

Vonnie Estes, PMA:
Great. All right. Thank you very much. Bill Danker, AgTech, SAS: You're welcome.

Vonnie Estes, PMA:
This is been eye-opening for me to learn about both how bad threat actors can

be, but also how easy it is to block a good majority of the threats. Hope this was helpful. See you next time.

Vonnie Estes, PMA:
That's it for this episode of PMA Takes on Tech. Thanks for allowing us to serve as your guide to the new world of produce and technology. Be sure to check out all our episodes at pma.com and wherever you get your podcasts. Please subscribe and I would love to get any comments or suggestions of what you might want me to take on. For now, stay safe, eat your fruits and vegetables, and we will see you next time.