How Florida School District Tames the Wild West of Education Security at Scale and On Budget

Transcript of a discussion about how a large public school system creates a new culture of computing safety at low cost and high scale.

Listen to the podcast. Find it on iTunes. Get the mobile app. Download the transcript. Sponsor: Bitdefender.

Dana Gardner: Welcome to the next edition of BriefingsDirect. I'm **Dana Gardner**, Principal Analyst at **Interarbor Solutions**, your host and moderator.

Bringing a central IT focus to large public school systems has always been a challenge, but bringing a security focus to thousands of PCs and devices has been compared to bringing law and order to the Wild West.

For the Clay County School District in Florida, a team of IT administrators is grabbing the bull by the horns nonetheless to create a new culture of computing safety -- without breaking the bank.

Today's BriefingsDirect security insight's discussion examines how Clay County is building a secure posture for their edge, network, and data centers while allowing the right mix and access for exploration necessary in an educational environment.

To learn how to ensure that schools are technically advanced and secure at low cost and at high scale, please join me now in welcoming Jeremy Bunkley, Supervisor of the Clay County School District Information and Technology Services Department.

Jeremy Bunkley: Pleasure to speak with you today, Dana.

Gardner: We are also here with Jon Skipper, Network Security Specialist at the Clay County School District.

Skipper

Jon Skipper: Thanks, Dana. I appreciate it.

Perkins

Gardner: Lastly, we are here with Rich Perkins, Coordinator for Information Services at the Clay County School District.

Rich Perkins: Thanks, Dana. Good to be here.

Gardner: Jeremy, what's been the biggest challenge to improving security, compliance, and risk reduction there at the school district?

Change is hard

Bunkley: I think the answer actually scales across the board. The problem even bridges into businesses. It's the culture of change -- of making people recognize security as a forethought, instead of an afterthought. It has been a challenge in education, which can be a technology laggard.

Getting people to start the recognition process of making sure that they are security-aware has been quite the battle for us. I don't think it's going to end anytime soon. But we are starting to get our key players on board with understanding that you can't clear-text Social Security numbers and credit card numbers and personally identifiable information (PII). It has been an interesting ride for us, let's put it that way.

Gardner: Jon, culture is such an important part of this, but you also have to have tools and platforms in place to help give reinforcement for people when they do the right thing. Tell us about what you have needed on your network, and what your technology approach has been?

Skipper: Education is one of those weird areas where the software development has always been lacking in the security side of the house. It has never even been inside the room. So one of the things that we have tried to do in education, at least with the Clay County School District, is try to modify that view, with doing change management. We are trying to introduce a security focus. We try to interject ourselves and highlight areas that might be a bad practice.

Education is one of those weird areas where the software development has always been lacking in the security side of the house.

One of our vendors uses plain text for passwords, and so we went through with them and showed them how that's a bad practice, and we made a little bit of improvement with that.

I evaluate our policies and how we manage the domains, maybe finding some stuff that came from a long time ago where it's no longer needed. We can pull the information out, whereas before they put all the Social Security numbers into a document that was no longer needed. We have been trying really hard to figure that stuff out and then to try and knock it down, as much as we can.

Access for all, but not all-access

Gardner: Whenever you are trying to change people's perceptions, behaviors, culture, it's useful to have both the carrot and a stick approach.

So to you Rich, what's been working in terms of a carrot? How do you incentivize people? What works in practice there?

Perkins: That's a tough one. We don't really have a carrot that we use. We basically say, “If you are doing the wrong things, you are not going to be able to use our network.” So we focus more on negatives.

The positives would be you get to do your job. You get to use the Internet. We don't really give them something more. We see security as directly intertwined with our customer service. Every person we have is our customer and our job is to protect them -- and sometimes that's from themselves.

Either you are a student and you get this level of access, or you are a staff member, you get this level of access, or you don’t get access.

So we don't really have a carroting type of system. We don't allow students to play games if they have no problems. We give everybody the same access and treat everybody the same. Either you are a student and you get this level of access, or you are a staff member, you get this level of access, or you don't get access.

Gardner: Let’s get background on the Clay County School District. Tell us how many students you have, how many staff administrators, the size and scope of your school district?

Bunkley: Our school district is the 22nd largest in Florida, we are right on the edge of small and medium in Florida, which in most districts is a very large school district. We run about 38,500 students.

And as far as our IT team, which is our student information system, our Enterprise Resource Planning (ERP) system, security, down to desktop support, network infrastructure support, our web services, we have about 48 people total in our department.

Our scope is literally everything. For some reason IT means that if it plugs into a wall, we are responsible for it. That's generally a true statement in education across the board, where the IT staff tends to be a Jack-of-all-trades, and we fix everything.

Practical IT

Gardner: Where you are headed in terms of technology? Is there a one-to-one student-to-device ratio in the works? What sort of technology do you enable for them?

Bunkley: I am extremely passionate about this, because the one-to-one scenario seems to be the buzzword, and we generally despise buzzwords in this office and we prefer a more practical approach.

The idea of one-to-one is itself to me flawed, because if I just throw a device in a student's hand, what am I actually doing besides throwing a device in a student's hand? We haven't trained them. We haven’t given them the proper platform. All we have done is thrown technology.

And when I hear the terms, well, kids inherently know how to use technology today; it kind of just bothers me, because kids inherently know how to use social media, not

technology. They are not production-driven, they are socially driven, and that is a sticking point with me.

We are in fact moving to a one-to-one, but in a nontraditional sense. We have established a one-to-one platform so we can introduce a unified platform for all students and employees to see through a portaling system; we happen to use ClassLink, there are various other vendors out there, that's just the one we happen to use.

We have integrated that in moving to Google Apps for Education and we have a very close relationship with Google. It's pretty awesome, to be quite honest with you.

So we are moving in the direction of Chromebooks, because it's just a fiscally more responsible move for us.

Kids today know how to use social media, not technology. They are not production-driven, they are socially driven.

I know Microsoft is coming out with Windows 10S, it's kind of a strong move on their part. But for us, just because we have the expertise on the Google Apps for Education, or G Suite, it just made a lot of sense for us to go that direction.

So we are moving in one-to-one now with the devices, but the device is literally the least important -- and the last -- step in our project.

Non-stop security, no shenanigans

Gardner: Tell us about the requirements now for securing the current level of devices, and then for the new one. It seems like you are going to have to keep the airplane flying while changing the wings, right? So what is the security approach that works for you that allows for that?

Skipper: Clay County School District has always followed trends as far as devices go. So we actually have a good mixture of devices in our network, which means that no one solution is ever the right solution.

We have a good mixture of devices in our network, so no one solution is ever the right solution.

So, for example, we still have some iPads out in our networks, we still have some older Apple products, and then we have a mixture of Chromebooks and also Windows devices. We really need to make sure that we are running the right security platform for the full environment.

As we are transitioning more and more to a take-home philosophy -- and that's where we as an IT department are seeing this going – so that if the decision is made to make the entire student population go home, we are going to be ready to go.

We have coordinated with our content filter company, and they have some extensions that we can deploy that lock the Chromebooks into a filter situation regardless of their network. That's been really successful in identifying, maybe blocking students, from those late-night searches. We have also been able to identify some shenanigans that might be taking place due to some interesting web searches that they might do over YouTube, for example. That's worked really well.

Our next objective is to figure out how to secure our Windows devices and possibly even the Mac devices. While our content filter does a good job as far as securing the content on the Internet, it's a little bit more difficult to deploy into a Windows device, because users have the option of downloading different Internet browsers. So, content filtering doesn't really work as well on those.

I have deployed Bitdefender to my laptops, and also to take-home Apple products. That allows me to put in more content filtering, and use that to block people from malicious websites that maybe the content filter didn't see or was unable to see due to a different browser being used.

In those aspects we definitely are securing our network down further than it ever has been before.

Block and Lock

Perkins: With Bitdefender, one of the things we like is that if we have those devices go off network, we can actually have it turn on the Bitdefender Firewall that allows us to further lock down those machines or protect them if they are in an open environment, like at a hotel or whatever, from possible malicious activity.

And it allows us to block executables at some point. So we can actually go in and say, "No, I don't want you to be able to run this browser, because I can't do anything to protect you. Or I can't watch what you do, or I can't keep you from doing things you shouldn't do." So those are all very useful tools in a single pane of glass that we can see all of those devices at one time and monitor and manage. It saves us a lot of time.

We aim to defend our internal network while you are here and our network will extend directly down into the student and teacher's home.

Bunkley: I would follow up on that with a base concept, Dana, and our base concept is of an external network. We come from the concept of, we are an everywhere network. We are not only aiming to defend our internal network while you are here and maybe do some stuff while you are at our house, we are literally an externally built network, where our network will extend directly down into the student and teacher's home.

We have gone as far as moving everything we physically can out of this network, right down to our firewall. We are moving our domain controllers, external to the network to create literally an everywhere network. And so our security focus is not just internal, it is focused on external first, then internal.

Gardner: With security products, what have you been using, what wasn't working, and where do you expect to go next given those constraints?

No free lunch

Perkins: Well, we can tell you that “free” is not always the best option; as a matter of fact, it’s almost never a good option, but we have had to deal with it.

We were previously using an antivirus called Avast, and it’s a great home product. We found out that it has not been the best business-level product. It’s very much marketed to education, and there are some really good things about it. Transferring away from it hasn’t been the easiest because it’s next to impossible to uninstall. So we have been having some problems with that.

We have also tested some other security measures and programs along the way that haven’t been so successful. And we are always in the process of evaluating where we are. We are never okay with status quo. Even if we achieve where we want to be, I don't think any of us will be satisfied, and that’s actually something that a lot of this is built on -- we always want to go that step further. And I know that’s cliché, but I would say for an institution of this size, the reason we are able to do some of the stuff is the staff that has been assembled here is second to none for an educational institution.

So even in the processes that we have identified, which were helter-skelter before we got here, we have some more issues to continue working out, but we won’t be satisfied with where we are even if we achieve the task.

Skipper: One of the things that our office actually hates is just checking the box on a security audit. I mean, we are very vocal to the auditors when they come in. We don’t do things just to satisfy their audit. We actually look at the audit and we look at the intent of the question and if we find merit in it, we are going to go and meet that expectation and then make it better. Audits are general. We are going to exceed and make it a better functioning process than just saying, “Yes, I have purchased an antivirus product,” or “I have purchased x.” To us that’s unacceptable.

Bunkley: Audits are a good thing, and nobody likes to do them because they are time-consuming. But you do them because they are required by law, for our institution anyways. So instead of just having a generic audit, where we ignore the audit, we have adopted the concept of the audit as a very useful thing for us to have as a self-reflection tool. It’s nice to not have the same set of eyes on your work all the time. And instead of taking offense to someone coming in and saying, “You are not doing this good enough,” we have literally changed our internal culture here, audits are not a bad thing; audits are a desired thing.

Gardner: Let’s go around the table and hear how you began your journey into IT and security, and how the transition to an educational environment went.

IT’s the curriculum

Bunkley: I started in the banking industry. Those hours were crazy and the pressure was pretty high. So as soon as I left that after a year, I entered education, and honestly, I entered education because I thought the schedule was really easy and I kind of copped out on that. Come to find out, I am working almost as many hours, but that’s because I have come to love it.

This is my 17th year in education, so I have been in a few districts now. Wholesale change is what I have been hired to do, that’s also what I was hired here to do in Clay.

We want to change the culture, make IT part of the instruction instead of a separate segment of education.

We have to be interwoven into everything, otherwise we are going to be on an island, and the last time I heard the definition of education is to educate children. So IT can never by itself be a high-functioning department in education. So we have decided instead to go to instruction, and go to professional development, and go to administration and intervene ourselves.

Education is to educate children, so we have decided to go to instruction, professional development.

Gardner: Jon, tell us about your background and how the transition has been for you.

Skipper: I was at active-duty Air Force until 2014 when I retired after 20 years. And then I came into education on the side. I didn't really expect this job, wasn't mentally searching for it. I tried it out, and that was three years ago.

It's been an interesting environment. Education, and especially a small IT department like this one, is one of those interesting places where you can come and really expand on your weak areas. So that's what I actually like about this. If I need to practice on my group policy knowledge, I can dive in there and I can affect that change. Overall this has been an effective change, totally different from the military, a lot looser as far as a lot of things go, but really interesting.

Gardner: Rick, same question to you, your background and how did the transition go?

Perkins: I spent 21 years in the military, I was Navy. When I retired in 2010, I actually went to work for a smaller district in education mainly because they were the first one to offer me a job. In that smaller district, just like here, we have eight people doing operations, and we have this big department. Jeremy understands from where he came from. It was pretty much me doing every aspect of it, so you do a little security, you do a little bit of everything, which I enjoyed because you are your own boss, but you are not your own boss.

You have to be flexible because education is not the military, so you can't be that stringent. That's a challenge.

You still have people residing over you and dictating how you are going to work, but I really enjoyed the challenge. Coming from IT security in the military and then coming into education, it's almost a role reversal where we came in and found next to no policies.

I am used to a black-and-white world. So we are trying to interject some of that and some of the security best practices into education. You have to be flexible because education is not the military, so you can't be that stringent. So that's a challenge.

Gardner: What are you using to put policies in place enforce them? How does that work?

Policy plans

Perkins: From a [Microsoft] Active Directory side, we use group policy like most people do, and we try and automate it as much as we can. We are switching over, on the student side, very heavily to Google. They effectively have their own version of Active Directory with group policy. And then I will let Jon speak more to the security side though we have used various programs like PDQ for our patch management system that allows us to push out stuff. We use some logging systems with ManageEngine. And then as we have said before we use Bitdefender to push a lot of policy and security out as well, and we've been reevaluating some other stuff.

We also use SolarWinds to monitor our network and we actually manage changes to our network and switching using SolarWinds, but on the actual security side, I will let Jon get more specific for you.

Skipper: When we came in … there was a fear of having too much in policy equated to too much auditing overhead. One of the first things we did was identify what we can lock down, and the easiest one was the filter.

One of the first things we did was identify what we can lock down, and the easiest one was the filter.

The content filter met such stipulations as making sure adult material is not acceptable on the network. We had that down. But it didn't really take into account the dynamic of the Internet as far as sites are popping up every minute or second, and how do you maintain that for unclassified and uncategorized sites?

So one of the things we did was we looked at a vendor, like, okay, does this vendor have a better product for that aspect of it, and we got that working, I think that's been working a lot better. And then we started moving down, we were like, okay, cool, so now we have content filtering down, luckily move on to active network, actually not about finding someone else who is doing it, and borrowing their work and making their own.

We look into some of the bigger school districts and see how they are doing it. I think Chicago, Los Angeles. We both looked at some of their policies where we can find it. I found a lot of higher education in some of the universities. Their policies are a lot more along the lines of where we want to be. I think they have it better than what some of the K-12s do.

So we have been going through there and we are going to have to rewrite policy – we are in an active rewrite of our policies right now, we are taking all of those in and we are looking at them, and we are trying to figure out which ones work in our environment and then make sure we do a really good search and replace.

Gardner: We have talked about people, process and technology. We have heard that you are on a security journey and that it's long-term and culturally oriented.

Let's look at this then as to what you get when you do it right, particularly vis-à-vis education. Do you have any examples of where you have been able to put in the right technology, add some policy and process improvements, and then culturally attune the people? What does that get for you? How do you turn a problem student into a computer scientist at some point? Tell us some of the examples of when it works, what it gets you.

Positive results

Skipper: When we first got in here, we were a Microsoft district. We had some policies in place to help prevent data loss, and stuff like that.

One of the first things we did is review those policies and activate them, and we started getting some hits. We were surprised at some of hits that we saw, and what we saw going out. We already knew we were moving to the Google networks, continuing the process.

We researched a lot and one of the things we discovered is that just by a minor tweak in a user's procedures, we were able to identify that we could introduce that user to and get them used to using email encryption, for example. With the Gmail solution, we are able to add an extension, and that extension actually looks at their email as it goes out and finds keywords -- or it may be PII -- and automatically encrypt the email, preventing those kinds of breaches from going out there. So that's really been helpful.

As far as taking a student who may be on the wrong path and reeducating them, Bitdefender has helped.

As far as taking a student who may be on the wrong path and reeducating them and bringing them back into the fold, Bitdefender has actually helped out on that one.

We had a student a while back who went out to YouTube and find out how he could just do a simple search on how to crash the school network, and he found about five links. And he researched those links and went out there and found that this batch filed with this type will crash a school server.

He was able to implement it and started trying to get that attack out there, and Bitdefender was able to actually go out there and see the batch file, see what it did and prevent it. By quarantining the file, I was able to get that reported very quickly from the moment that he introduced the attack, and it identified the student and we were able to sit down with the administrators and talk to the student about that process and educate them on the dangers of actually attacking a school network and the possible repercussions of it.

Gardner: It certainly helps when you can let them know that you are able to track and identify those issues, and then trace them back to an individual. Any other anecdotes about where the technology process and people have come together for a positive result?

Applied IT knowledge for the next generation

Skipper: One of the things that's really worked well for the school district is what we call Network Academy. It's taught by one of our local retired master chiefs, and he is actually going in there and teaching students at the high school level how to go as far as earning a *Cisco Certified Network Associate (CCNA*)-level IT certificate.

If a student comes in and they try hard enough, they will actually figure it out and they can leave when they graduate with a CCNA, which is pretty awesome. A high school student can walk away with a pretty major industry certification.

A high-school student can graduate and walk away with a CCNA, which is a major industry certification.

We like to try and grab these kids as soon as they leave high school, or even before they leave high school, and start introducing them to our network. They may have a different viewpoint on how to do something that's revolutionary to us.

But we like having that aspect of it, we can educate those kids who are coming in and getting their industry certifications, and we are able to utilize them before they move on to a college or another job that pays more than we do.

Bunkley: Charlie Thompson leads this program that Jon is speaking of, and actually over half of our team has been through the program. We didn't create it, we have just taken advantage of the opportunity. We even tailor the classes to some of the specific things that we need. We have effectively created our own IT hiring pipeline out of this program.

Gardner: Next let's take a look to the future. Where do you see things going, such as more use of cloud services, interest in unified consoles and controls from the cloud as APIs come into play more for your overall IT management? Encryption? Where do you take it from here?

Holistic solutions in the cloud

Bunkley: Those are some of the areas we are focusing on heavily as we move that "anywhere network." The unified platform for management is going to be a big deal to us. It is a big deal to us already. Encryption is something we take very seriously because we have a team of eight protecting the data of about 42,000 users..

If you consider the perfect cyber crime reaching down into a 7th or an 8th grader and stealing all of their personal information, taking that kid's identity and using it, that kid won't even know that their identity has been stolen.

We consider that a very serious charge of ours to take on. So we will continue to improve our protection of the students' and teachers' PII -- even if it sometimes means protecting them from themselves. We take it very seriously.

As we move to the cloud, that unified management platform leads to a more unified security platform. As the operating systems continue to mature, they seem to be going different ways. And what's good for Mac is not always good for Chrome, is not always good for Windows. But as we move forward with our projects we bring everything back to that central point -- can the three be operated from the single point of connection, so that we can save money moving forward? Just because it's a cool technology and we want to do, it doesn't mean it's the right thing for us.

Sometimes we have to choose an option that we don't necessarily like as much, but pick it because it is better for the whole. As we continue to move forward, everything will be focused on that centralization. We can remain a small and flexible department to continue making sure that we are able to provide the services needed internally as well as protect our users.

Skipper: I think Jeremy hit it pretty solid on that one. As we integrate more with the cloud services, Google, etc., we are utilizing those APIs and we are leading our vendors that we use and forcing them into new areas. Lightspeed, for instance, is integrating more-and-more with Google and utilizing their API to ensure that content filtering -- even to the point of mobile device management (MDM) that is more integrated into the Google and Apple platforms to make sure that students are well protected and we have all the tools available that they need at any given time.

We are really leaning heavily on more cloud services, and also the interoperability between APIs and vendors.

We are leaning heavily on more cloud services and the interoperability between APIs and vendors.

Perkins: Public education is changing more to the realm of college education where the classroom is not a classroom -- a classroom is anywhere in the world. We are tasked with supporting them and protecting them no matter where they are located. We have to take care of our customers either way.

Gardner: I'm afraid we'll have to leave it there. You've been listening to a sponsored BriefingsDirect discussion on how Clay County is building a secure posture for their edge, network and data centers while allowing the right mix of access and exploration necessary in an educational environment.

And we have learned how bringing a security focus to thousands of PCs and devices can ensure that schools are technically advanced and secure at low cost and at high scale.

So please join me now in thanking our guests, Jeremy Bunkley, Supervisor of the Information and Technology Services Department; Jon Skipper, Network Security Specialist, Rich Perkins, Coordinator of Information Services, all at the Clay County School District in Florida.

This is Dana Gardner, Principal Analyst at Interarbor Solutions, your host and moderator for this ongoing series of BriefingsDirect discussions. A big thank you to our sponsor, Bitdefender, for supporting these presentations, and also a big thank you to our audience for joining us. Do come back next time.

Listen to the podcast. Find it on iTunes. Get the mobile app. Download the transcript. Sponsor: Bitdefender.

You may also be interested in:

- The next line of defense—How new security leverages virtualization to counter sophisticated threats
- How IT innovators turn digital disruption into a business productivity force multiplier
- Cybersecurity standards: The Open Group explores security and safer supply chains
- How the Citrix Technology Professional Program Produces User Experience Benefits from Greater Ecosystem Collaboration
- DevOps and Security, a Match Made in Heaven
- Expert Panel Explores the New Reality for Cloud Security and Trusted Mobile Apps Delivery
- Cybersecurity crosses the chasm: How IT now looks to the cloud for best security
- Capgemini and HPE Team Up to Foster Behavioral Change That Brings Better Cyber Security Across Application Lifecycles
- Feedback loops: The confluence of DevOps and big data