# **The Digital Aspirations in Business Podcast S2E5 (transcript)**

**Building Foundational Elements of Security for K12s and SMBs**

*Securing your business from breaches, ransomware and other security threats*

Doug Stevens and Michael O’Connell at Aspire Technology Partners

**Doug Stevens:** Hello and welcome to Season 2, Episode 5 of the Digital Aspirations in Business podcast series. My name is Doug Stevens, and I'll be your host today. If you're not aware, October is National Cybersecurity Awareness month. So, we thought, what better time than to dedicate this podcast to helping our listeners to secure their businesses from breaches, ransomware, and other security threats.

**Doug Stevens:** And today, we're really going to focus around small and mid-sized organizations. They have some unique challenges. A lot of times there's limited resources, especially from a security perspective. Security analysts and engineers are expensive. They're hard to find. They're hard to keep. So, what we found in these types of organizations is IT folks are wearing multiple hats. Maybe they're the network guy or the system's guy, but they're also the security person. They have multiple responsibilities.

**Doug Stevens:** The challenge becomes very difficult to keep up. The threats are constantly evolving. Again, you're wearing multiple hats. The attack surface has changed dramatically over the last 18 months with COVID, and work from home, and this acceleration of companies and their cloud adoption. So, when we talk to customers - and we talk to a lot of them every day - they're really looking for help and they're looking for guidance.

**Doug Stevens:** And what we try to do in a mid-sized organization is try to make it simple and actionable. And try to suggest maybe four or five technologies that an organization can implement that would have a really dramatic improvement on their overall security posture. And without introducing a ton of complexity or effort from an implementation perspective.

**Doug Stevens:** So, we're calling this podcast our Foundational Elements of Security. And it's going to be applicable to any size organization, but I think it's nicely suited whether your K through 12, or an SMB, or a mid-sized enterprise. Everything we're going to talk about today is cloud-delivered. It doesn't require a lot of effort and it's easy to consume.

**Doug Stevens:** So, to help me today, I'd like to introduce Michael O'Connell. Michael is a Solutions Architect within Aspire cybersecurity practice. He has a ton of experience, both on the pre-sale side with consulting, as well as very hands-on in field implementations and service delivery. He's got a wide variety of expertise across multiple security technologies and manufacturers. Welcome to the podcast, Michael.

**Michael O'Connell:** Thank you, Doug. Thank you for the introduction. As you said, my name is Michael O'Connell. I'm the Security Solutions Architect here at Aspire. I have over 15 years of experience, both in pre-sales and post-sales across many different vendors. I look forward to the podcast today.

**Doug Stevens:** Awesome. I appreciate it. I should also mention, too, that Michael is a die-hard Philly sports fan and a die-hard hockey player. So, I've learned over the years, you don't mess with hockey players for a lot of reasons.

**Michael O'Connell:** I'm getting older but I still try, men's league and just try to stay active. And then, Philly sports aren't doing so well lately so that's a little painful.

**Doug Stevens:** Well, I can feel your pain. As a New York Football Giants fan and a Mets fan, we won't go. We'll focus on security today and that'll make us all a lot happier.

**Michael O'Connell:** Absolutely.

**Doug Stevens:** All right. So, let's jump into it. So, from a threat landscape perspective, you open up the news every day with what every company is dealing with is ransomware. It doesn't matter whether it's a commercial business, or it's the public sector, a small business, a large IT service provider, consultancy with a global footprint, it's completely random and it's happening more and more.

**Doug Stevens:** I was reading a report last week from the Treasury Department and it said that ransomware victims in the first six months of this year, 2021, paid a total of $590 million in ransomware. And so, when you compare that to all of 2020, that total was 416 million. So, in the first half of 2021, there's already been a 42 percent increase over the entire year in terms of ransomware payments. That's a huge number. That's something that keeps business owners and IT folks awake at night.

**Doug Stevens:** So, aside from the ransomware out there, Michael, what are some of the other most common exploits that you're seeing out in the field?

**Michael O'Connell:** So, there's a wide variety that are out in the field, and these are all going to fall under the umbrella of what I'm going to call and what in the industry we call malware. So, malware is kind of an inclusive term for all types of malicious software. So, one of the ones that you'll see on a daily basis, a lot of times that you get before the ransomware event starts with adware.

**Michael O'Connell:** Adware is legitimate. Maybe you go to a search engine or maybe you go to a news portal and you'll see some advertisements. That's called adware. But a majority of that out there is not legitimates. The purpose of that is to make unauthorized access to a computer system. And that is where a majority of your ransomware can get started if it's not devised in a phishing attack.

**Michael O'Connell:** The second one I would say is phishing. So, your users internally get an email. They think it's a legitimate email. It looks like it may come from someone in an organization or a trusted business partner. They click on that link, that then downloads an executable or it pulls down code from the internet from a phishing attack, which then can go ahead and escalate to a ransomware attack.

**Michael O'Connell:** The third one, I think, that a lot of people have kind of forgotten about, especially with a lot of the ransomware and the purpose of actually a criminal mastermind behind that gain financial incentive for locking you out of your systems is botnet. So, what is a botnet? Well, that's short for robot network. What is that? These are network infected computers under a single control of an attacking party. So, also known in the IT industry as command and control servers. Botnets are highly versatile and adaptable. What are these used for? These are used for DDOS or distributed denial-of-service attacks.

**Michael O'Connell:** So, it's a diverse playing field. Ransomware is the one that's always in the news, but I think the adware, the phishing, and the botnets are the other ones I like to focus on too.

**Doug Stevens:** That's interesting. Botnets have been around for a long time and they haven't been in the news as much as some of these other threats, until very recently. We've seen a lot of distributed denial-of-service attacks against some of the larger kind of cloud-based service providers out there.

**Michael O'Connell:** From a small business side, botnets are not highly as much utilized. Now, as your platform possibly goes more cloud-based or web service hosting, that's just something to keep in mind and just know that it is still out there. It's something that's not going away. Ransomware hasn't replaced it. So, I kind of just like to comment on that.

**Doug Stevens:** That's a great point. All right. Well, let's jump into it. So, the first in the foundational elements of security that I wanted to touch on - and I'll just sort of reiterate what our common ground rules for our podcast. We don't want to push specific products and we certainly want to be consultative when we're talking to our audience and when we're talking to potential customers on a daily basis. And this is just in my person - I think Cisco Umbrella is a tool that any organization should implement just from an ease-of-use perspective and the value that it provides. So, that first foundational level of security is DNS protection. So, Michael, what I would ask is, why is Umbrella so perfect for every organization and what's the value there?

**Michael O'Connell:** So, one of the biggest values right off the bat is, Umbrella gives the backend integration with Cisco Talos - and we won't speak to this vendor specifically right now at this moment. But what that does is gives you the ability to predict and block new malicious domains with machine learning. So, it's a dynamic update service. So, it's a cloud-based service so it's dynamically updating. Gone are the days where myself, as a security engineer, or my team, or the customers internal team, they're not going in and adding these manually.

**Michael O'Connell:** So, it's a dynamic block, especially with COVID and the hybrid workplace depending on what the small business and what your organization may be doing, it gives you the visibility and enforcement to be able to put corporate-wide policies no matter where that workstation is. That's not specific just to the umbrella platform. There's other ones that do that and we'll go into that in a little more detail. However, just regards that product, that's really a big adoption in 2020 and 2021 in just moving forward in the security landscape.

**Doug Stevens:** I just think from an ease of deployment standpoint, you're literally pointing DNS to new IP addresses. And within 20 minutes, you're getting DNS layer protection. You're able to apply policy across users, whether they're on the network or whether their remote. And all of that complexity is simplified because its cloud-based. And from a high impact without a lot of high cost, I just think that's a tremendous technology. So, number one is DNS layer protection.

**Doug Stevens:** And, now, we'll go back to not talking about specific products, but the second area of foundational element of security, for me, is endpoint protection. And endpoint protection has changed. It's not your traditional antivirus anymore. So, Michael help us, what's the role of endpoint protection? And why is it different from traditional AV?

**Michael O'Connell:** So, over the years it's changed dramatically. So, gone are the days where you're relying on a definition file, or in a lot of legacy times is known as a dot file. Where your IT staff has to pull that down and automatically update or push an update by a third party program or internal program to all your work stations. So, the biggest thing now from an endpoint protection is to have - what I kind of referred to a little bit earlier - dynamic analysis and auto-updates.

**Michael O'Connell:** So, for example, we're on the east coast in the United States. If there's an outbreak overnight in the middle of Europe or Asia, wherever the geographic region is. I'm asleep or your IT staff from a small business perspective is asleep. You don't have a 24/7, 365 SOC infrastructure there to monitor that. With a dynamic analysis and the way the endpoint protection suites work now, their job is to stop advanced threat. So, they're going to go ahead and dynamically update it.

**Michael O'Connell:** If you see a malicious actor, or files that maybe looked legitimate but are not, they've been submitted, your endpoints are going to dynamically update. So, when your user and your business critical application people open that laptop or that file in the morning, it's going to pull that down as soon as it gets internet access no matter where that's at.

**Michael O'Connell:** So, gone are the days of - what I'd like to call - antivirus. It's more about advanced malware protection at this point. So, the endpoint is not only going to use AV back integration, but it's also going to get the malicious and other third party threat grids into that product.

**Doug Stevens:** And just clarify for us if you would, too, please. Is there a behavioral element to this? Is it all signature-based? What's the neuro technology that these solutions are using?

**Michael O'Connell:** So, they use behavioral-based threat detection is what it's called. So, that can start all the way at the BIOS level, all the way into your endpoint detection and response. So, automatically it's an automation perspective. So, if they see a signature file that is correlated to maybe a malicious domain, or something I was referring to, something happen overseas overnight while I was asleep, automatically it's going to pull down the latest actual malicious files. And it's going to quarantine that where I don't actually have to go in and do it myself. So, it's fully automated, almost, from a full behavior and it's dynamically updating.

**Michael O'Connell:** For example two hours from now, there's another file, or an executable, or maybe a DLL file that changes, that endpoint is going to dynamically update based off your cloud service provider in order to download and protect your endpoint. So, it's absolutely behavior. You still set up some baseline configurations. However, majority of your protection is behavioral isolation-based.

**Doug Stevens:** And just to kind of put a bow on this, this particular technology at the endpoint layer, you're talking about laptops, you're talking about workstations, and servers as well, right?

**Michael O'Connell:** Depending on the product. The laptops, I'd like to get a little more granular. So, the Windows laptops, whether that's a MacBook, you can also do Chromebooks, if you have a K through 12 or maybe you have an educational facility. Some products can also support Chromebooks, which are relatively cheap and easy to deploy for a short period of time. Servers, obviously, whether that's domain controllers, file servers, web servers, whatever that is. You can even get as granular as into mobile devices protections, too, depending on the product you're looking at. But majority, yes, Doug, correct. Absolutely, we're talking laptops, MacBooks, servers and so forth and so on. The other ones are just additional options.

**Doug Stevens:** Got it. Awesome. All right. So, let's move ahead here. So, the third foundational element of security that I wanted to touch on with you, and this relates in what we've seen a lot especially this year, obviously with ransomware, we touched on it earlier, a lot of companies are trying to update their insurance policies by adding some sort of cybersecurity insurance to their existing business insurance. In the event that they get hit with ransomware, they have that protection.

**Doug Stevens:** And a lot of the insurance carriers now are much more, I would say, prescriptive in who their writing policy for. And they want to understand and they want to do an assessment of that business's security infrastructure prior to writing that policy. And one of the things that they, without any exception, are looking for is some sort of multi-factor authentication deployed in the environment. So, help us understand what MFA is and the role that it plays from a security perspective.

**Michael O'Connell:** So, MFA stands for multi-factor authentication, as you mentioned. So, what is multi-factor authentication? It's an authentication method that requires your user, your employee to provide two or more verification factors. So, not only do I have my standard login for your corporate organization. Whether that's your email, your VPN, maybe an application on the web, maybe a sales resource, accounting, however that application is, but it also adds an additional layer of security.

**Michael O'Connell:** So, there's multiple ways to do that. You can get a push to your smartphone. Nowadays, everybody really has a smartphone with them 24/7. So, you can set up a smartphone push. So, when I login as Michael O'Connell, not only do I log into my corporate resource, but then I get a push to my phone. We can add other additional options. But majority, as you mentioned, with the cybersecurity and insurance, two factors the very bare minimum that you want to implement. You can add three, four, five options. But the end goal is to add additional authentication methods. So, not only am I logging in as Michael O'Connell, but then I'm going to require a push to my phone.

**Michael O'Connell:** You can also do a hard token, if you don't want to implement, for example, smartphone integration. You can do text messages. You can also do phone calls. And some organizations and some places do additional email. If you're obviously logging into email, it gets a little tricky. But there's multiple options. So, at the end of the day, the goal is to provide two-step authentication to verify you are who you say you are.

**Doug Stevens:** And, again, just focusing on that mid-sized company or that K through 12, just having that capability and have it cloud-delivered and being able to verify the identity of the user and establish that device trust and really enable that secure access to critical applications. That's huge.

**Michael O'Connell:** Yes. That's absolutely the biggest edge threat defense. So, at the end of the day, if I have to have two points of authentication, it's going to give me an additional layer of protection.

**Doug Stevens:** And it's easy to use. I mean, we use it internally. It's so easy. It's a couple of seconds, a couple of pushes, and you're in. But it makes a tremendous difference.

**Doug Stevens:** So, let's jump to the fourth element of foundational security, and this one touches on some of the phishing and the other threats that you had mentioned earlier. And it's so critical in helping a company's users be an additional kind of line of defense. And that's security awareness training. So, Michael, talk to us a little bit about what security awareness training is, how it's delivered, and what the benefit is to the organization.

**Michael O'Connell:** Perfect. Absolutely. So, the number one thing is, I mentioned earlier, about a phishing attack. Maybe somebody receives an email and it seems like a C-level executive in your organization may have wrote that email. That's not actually from them. So, the number one line of defense and, in my opinion, one of the most critical cybersecurity components is training of the security awareness. So, the first thing is to teach them what a phishing looks like, what you're looking for in an email.

**Michael O'Connell:** So, if I'm an end user and my user sees an actual email comment. It looks like it's from there. But really if they click on the actual details of the message, they'll be able to see maybe it's from a Gmail account. It's not from a corporate. So, there's one prime example from a phishing perspective. But we're also talking about clicking on actual links, looking at ads, shopping. Especially when you're talking about rolling into the holiday seasons, there's going to be a ton of adware, I mentioned earlier, on websites.

**Michael O'Connell:** Just going over a holistic overview of what not to do on your corporate resources compared to what you may want to do at your home. There's different areas and different times for different shopping, or supposed to be doing things for your organization. So, I think it's a hybrid model. It's based off each individual organization. So, K through 12 may have a different security awareness curriculum around their individual applications. But I think it's important to hybrid internet browsing, social media networking, ads, and also email awareness for adware or phishing.

**Doug Stevens:** Absolutely. And most of these solutions have a library of content. So, different on demand videos for the training piece. You can launch phishing attacks internally and test how people react to them. If someone fails, or they click on something, you can kind of direct them back for additional training. And it just provides that ongoing touch point over the course of a year just to remind the users, "Hey, it's important for you to be very skeptical and have your eyes open. And don't click on things that you're not aware come from someone you know."

**Michael O'Connell:** Absolutely. Just like you mentioned, I think it's very important to focus on doing the internal training. So, sending out those fake emails or sending out those fake links, there's no shame in someone clicking on it. It's just only going to improve your security posture and the training at the end of the day. So, I absolutely recommend doing that whether that's a 30 day basis, whether that's quarterly, however the organization is structured, definitely develop a plan for that.

**Doug Stevens:** It's so important, not expensive, very actionable. Every organization should be doing this on a regular basis. And this is kind of the fifth, and we'll try to tie this up a little bit here. But the fifth area that, I think, gets overlooked a lot, especially mid-sized companies with some challenges from a resourcing perspective, that's having the ability to be looking at security events and responding to alerts in any sort of regular way.

**Doug Stevens:** And, again, folks internally having multiple responsibilities and kind of focused in other areas. And what we found happens is that, the tools that are in place are doing their job. They are learning when they see something. But in some of these cases, when companies aren't looking at those alerts or responding to them, they get missed, they don't get addressed. And that problem grows and grows and grows until you have either a breach or some sort of ransomware event and it becomes a huge problem. So, could you talk to the importance of security event monitoring and maybe the role that an MSSP can play in helping customers address that area of need.

**Michael O'Connell:** So, number one, looking at previous experience, I've worn many different hats at many different organizations, especially in the post-sales role world. I can say, full disclosure, I did not monitor my tools 24/7, 365. As I mentioned earlier, I have to sleep a little bit every once in a while. So, what an MSSP and what a platform can do for you there, number one, they're trained specifically on the actual malware and malicious threats. They are well-aware and well- versed. They are 24/7, 365 staffed. Someone's going to be able to look at your alerts. When they see an alert come in, they're going to immediately be able to respond to it. What I like to call that is instant response. So, they're structured. They have a methodology for handling all cybersecurity incidents, any threats.

**Michael O'Connell:** In endpoint, for example, has a malicious actor where a file downloaded. They'll be able to go ahead and isolate or quarantine that. Make sure it doesn't spread through your infrastructure. Like we mentioned earlier, if you have a DNS malicious outbound look up. So, you have a server, for example, all of a sudden starts sending 3000 alerts out. So, bad actor websites that are known flag, they'll be able to stop and integrate in that. That can all happen within two hours at 3:00 in the morning on a Monday morning while I'm asleep.

**Michael O'Connell:** So, within MSSP and a 24/7, 365 staff, number one, I think you focus on that's their job, 24/7, 365. They are constantly protecting and looking after your corporate assets. They're trained. That is what they do. Not wearing multiple hats. They're responding to the incidents. And more importantly, you always want to be able to work with them and develop an incident response plan or an IRP. So, you can efficiently identify and minimize any damage, reduce the cost of any kind of attack vector in your infrastructure. And I think within MSSP, you're going to gain all of that without having to have a dedicated set of a SOC or analyst 24/7, 365.

**Doug Stevens:** I totally agree. And, really, when you look at it from an economy of scale standpoint and investment standpoint, most companies, they don't have the budget and the wherewithal to build their own SOC or hire a security analyst or to implement a sim. It just makes so much more sense to leverage an MSSP for a fraction of the cost of adding one additional full-time employee you can get 24 by 7 threat monitoring and response capabilities.

**Doug Stevens:** And you can get those response playbooks for, "Hey, if we see this, then take these steps." And all of that technology and all the platforms, just from a security maturity perspective, it just happens overnight. So, just a ton of value there.

**Michael O'Connell:** And those teams are always training. They're constantly being updated on the newest tool sets. And as I said, they're not wearing multiple hats, they're experts in that area. So, I absolutely agree, it's worth the investment 100 percent.

**Doug Stevens:** All right. Well, we're coming to the end of our allotted time here. I hope this was helpful. What we tried to do today was to focus on a few actionable areas of security. Those foundational elements that we've been referring to. We've emphasized a lot around cloud- delivered for simplicity.

**Doug Stevens:** And so, just to sort of reiterate, that first one was DNS layer protection. Second is endpoint protection. Endpoint detection and response is kind of that product category that is evolving today. The third is multi-factor authentication and having that capability to verify users and establish that device trust. The fourth we talked about was security awareness training and just being able to educate our users to be that line of defense that will play a huge role in helping us to improve our security posture.

**Doug Stevens:** So, just closing thoughts for me, my recommendation would be, go out and find a good security partner. Seek their guidance. Do an assessment. Focus on those areas of high risk. And build a road map. You don't have to do all of this overnight. It can be a lot. Security is a journey. So, focus on that the areas of a high-risk and build a plan, and go down that path. And at the end of the day, what we're trying to do is we're trying to balance risk and cost and do what makes sense from a security perspective for the overall business. Those are my thoughts, Mike, any closing thoughts for you?

**Michael O'Connell:** No. I think that you covered everything. The only thing I would probably add is, when you're looking at a security partner, ask for demos, ask for proof of values, or proof of concept. See how it would work in your infrastructure. That provides a large value for you to go ahead and try before you buy. Being able to see and interact with them, I think that that'll give you a good overview of the services you're going to receive.

**Doug Stevens:** Actually, that's a great point. Again, it feeds off of what we've been talking about. A lot of these solutions are cloud-delivered. So, a good MSSP or a good security partner is going to be able to quickly stand up free trials and proof of concepts. And talk about, "Hey, what are you looking to do? What are the areas that you're looking to address? Let us show you what the tool will do in your environment." And then, make a decision from there. So, great advice.

**Doug Stevens:** Mike, thank you very much for being with us today. We appreciate all of your input. To our listeners, if you like the discussion today and you like to hear more, please go to our website, aspiretransforms.com and click on additional podcasts. As always, thank you for listening. And we'll see you next time on Digital Aspirations for Business. I'm your host, Doug Stevens. Bye for now.

**Outro:** Digital Aspirations is brought to you by Aspire Technology Partners, a premier technology solutions and services provider designing, implementing, delivering, and managing digital infrastructure and IoT solutions to enable transformational business outcomes, creating more agile and efficient IT environments that deliver differentiated customer experiences for your organization. To learn more about Aspire Technology Partners, visit aspiretransforms.com or email us at podcast@aspiretransforms.com.