Richard interviewed Bob Kocis (CRO), Michael George (CEO) and Fielder Hiss (VP of Product) of the Continuum Executive Board during their Navigate Conference in Boston in September this year.

Bob Kocis

RT: You're the second-ever returning guest to the podcast! I want to talk about leadership with you, but there's also been so much coming out of the Navigate event that it's hard to know where to start. Let me ask you: what do you think is the biggest thing you want MSPs (managed service providers) to pay attention to from Navigate?

BK: I think MSPs that are engaged with Continuum have what I call a 'first mover advantage.' Jay Ryerse from Carvir did a nice job of building the company as being by an MSP and for an MSP, and I think that's unique. Most of the other players come from the enterprise or another area, and they don't really understand the MSP market.

We recognise that, and we brought Jay into the fold and did the Carvir acquisition, which was very strategic for us. It allows us to enable the MSPs to have a complete security portfolio, and it allows them to get off the ground and running. Yes, you're going to have to train your internal resources and you might hire some folks, but with minimal investment you

can go ahead and really add value to your client base, so I think that's the big takeaway from this.

RT: During his keynote, Michael talked about the importance of MSPs needing to pivot. I'm a former MSP owner, and he's absolutely right – in the last 20 years I can see two or three times that I pivoted.

How are you helping MSPs to adapt? The reason I ask that question is because I think security plays a big part in that, doesn't it?

BK: It really does. You probably heard this on the CEO panel today, but I think they nailed it. It's a daunting task to think that you need to go and build your own security operation centre. It could even be a daunting task to think about hiring one or two security experts that operate at very high level.

What we're trying to do for MSPs is to bring that competency to them in an organised fashion with all the processes, the right technology and all the things they need to successfully service their clients. I think that's something that's unique to us and something that's going to be really impactful for the MSP, and allow them to make the pivot truly into cybersecurity.

RT: Just before we came on air, you and I were talking about the skills shortage and how Continuum, I won't say negates the need, but helps reduce the need to hire more and more people. It doesn't replace the need though, so can you talk about that and how you're seeing Continuum partners and how they're dealing with that?

BK: We're seeing folks that embrace our platform, their headcount will still grow over time and their business grows rapidly. But their employees are on higher-value-added roles. They're doing strategic consulting with their clients, they're working on strategic projects, helping develop new business and opportunities and helping the company pivot to great marketing opportunities like security.

They're not doing the day to day, mundane tasks that we're automating through our system and through our RMM (remote monitoring and management) agents. That's the big thing that we're seeing out there in the market, and we want to make sure that MSPs understand that.

We're not necessarily there to replace staff, although we might be replacing a function that's done today, but those employees are very valuable, and we get that. We want those employees to take higher-added-value roles in the organisation.

RT: Continuing on the theme of security – we're now in a world where cybercrime now exceeds all other forms of crime. That's slightly scary, but by the same token, I'm going to guess with your sales hat on, you also see that as an opportunity for MSPs.

BK: It's a great opportunity**.** The one thing I see coming out of it, and I'll take a different tack than other folks would on this question, but I see an opportunity for the MSP to really paint a picture for the client on how they're protected today, and then explain things to them.

There's a new threat every day. There're new things happening – viruses, phishing, attacks, and all these are happening in real time. It's impossible for an MSP to protect on everything that happens with the old way that we protected.

Once you paint that picture and you say, 'Look, we're protecting you with five or six items today, but there are these others that are open'. We want to make sure that they can communicate that with the client, and then communicate that they have offerings backed by Continuum that they can share with the client so they can solve those problems.

RT: We've heard the term 'Managed Service Security Provider' – MSSP, another acronym. I know how to define an MSP, so how would you define an MSSP?

BK: An MSSP is typically only focused on helping on the security front. They're not doing the traditional work that a managed service provider has done. You'll see a lot of MSSPs operating in a larger category of space, where a company already has an IT department but they don't have security expertise, so they bring in an MSSP.

Continuum is a good example: for many years of our growth we had IT staff, but we didn't have a CSO (chief security officer) because we had an MSSP in the background, and many companies operate that way.

I think there's a bit of a difference there, because MSSPs are very specialist, and we don't see them operating a lot in our space. When you think about employee accounts that we're trying to service – 250 and below, that really don't have an IT staff - we don't see that.

But I think the need for our MSPs to also be considered an MSSP is critical, because a small business doesn't want to go to two suppliers, and the MSP is poised to make that shift and become an MSSP.

I think it was Joe Panettieri who said, 'It's going to be one word.' Those terms are going to merge, and I think what we're going to see out of that is that we're going to be able to provide the ability for them to pivot and provide both services to the small medium business client.

RT: Let's pivot the conversation a little bit. You and I have spoken about leadership before, and I'd say you're a student of leadership technique. I read a brilliant article you put together, a summary of Jocko Willink's presentation and I encourage listeners to seek that one out.

There are a lot of business leaders and MSP owners here at Navigate. What advice do you give them to be not just good, but great, leaders?

BK: It's a great question, and I think there are a couple of things. One of the things that Michael George does, and I'll speak about him as a leader because I work with him every day, is he pushes us to stay ahead of the curve. I think the MSPs I see that are growing really rapidly, and they're worried about taking their clients ahead of the curve, and I think that's really important from a vision standpoint.

The second thing is, they never shy away from value and they're not out there selling on price. The MSPs are out there leading, and they're telling the client, 'I'm going to be more expensive, but there's a reason why. You have problems now that I'm going to fix for you and I'm going to make sure you're not having them anymore.'

I think having the confidence, from the CEO position of the MSP, and the leadership to say, 'We're going to charge a premium, but you're going to get world-class service and we're going to make sure we're going to take care of you,' which is what great leaders do, is an important element as the MSPs have to pivot.

One of the largest objections we get in security is that our clients already believe we have security, so they're not going to want to buy different security products. But the reality is, the clients know they've been protected, but they don't necessarily know all the things that are going on in the market. Once you educate them, they open up.

They say, 'OK, we get it. You guys have done a certain amount, but we should be protecting these other areas.' So just providing that thought leadership, the ability to sell on value and making sure you don't undercut your prices is really important.

RT: And again, a shout-out for the stuff that you share on LinkedIn. I'd recommend to listeners to follow Bob on LinkedIn. Talking of confidence, we're going to see the 'MSP Shark Tank' later on today, where MSPs pitch their security ideas. How would you catch the judges' attention if you were pitching?

BK: I think there are a couple of things I would do. One is: there are a lot of people out there selling security, and everyone has a flavour of it, whether you're just doing endpoint DNS (Domain Name Server) or you're doing something really advanced. I think the people that are differentiating themselves are the people that are really becoming consultative in their approach, and educating the business consumer on where they're vulnerable.

Someone at the CEO panel made the point today I really loved: "Look, we're not going to sell to the market by scaring them, because we're not insurance salespeople. We need to explain to them that for business continuity reasons and to run their business in a safe manner to protect their end customers, to sell security in that way."

So that would be my coaching advice – to make sure a company is positioning cyber-security as something that's going to add real value to the clients, rather than selling it on 'the sky is falling.'

RT: For anybody listening in the UK, Shark Tank is an American show, and the closest analogy in the UK would be Dragon's Den. You've had some changes in the UK office leadership. Can you give us any updates on plans for Europe? I imagine there are some exciting things around the corner?

BK: There is, and unfortunately, I can't tell you who or when, but I can tell you that I've been working hard on a process to find a new managing director for Europe. It's been a great search process, and I've met with a tremendous amount of people who really would like to

join Continuum. There is a certain skillset that you're looking for in a managing director, and I think we're close.

Before Christmas we should have somebody announced and I'm excited for that next chapter. I think our previous leader did a great job of getting us to a certain point and built up a really good business, and I really appreciate the efforts of the current team and also our clients.

RT: We're going to have a Navigate Europe or UK user group event again next year?

BK: Yes, we'll be having Partner Day. We haven't set the date yet, but we'll be having a small version of Navigate that we do in the UK, and we're thinking about extending it to a day and a half – we're going to solicit some survey data from the UK partners as we're thinking a half day of training at the back end could be valuable if they bring us the topics they want us to do. We're excited to set that up and I think it'll be really valuable.

RT: And hopefully we can get you across again and you can do another interview for the podcast and you'd be the first twice-returning guest and overtake Phylip Morgan.

BK: I'd appreciate the chance to overtake Phylip Morgan!

RT: Have you got any messages for UK MSPs, to do with Continuum or the wider MSP industry?
BK: My message would be this: Now we're going live with security and it's GDPR compliant, I think we've done a nice job in the UK and Benelux in serving our clients properly with RMM, and the entire technical team did a nice job of onboarding our clients. We're giving good value and getting good survey results and people are liking what they're seeing.

The next wave of this, with security, is such an opportunity. What we're doing is taking enterprise-grade solutions, like Sentinel One, like Event Tracker and bringing them to the SMB, and we're also bringing all the service work you need to make that happen.

My advice would be, build a security game plan. We would love to help you if we can and be part of that, and then engage our team as we're happy to share all of the expertise we have in helping you build that plan.

Fielder Hiss

RT: Fielder, what's your job title?

FH: I'm Vice President of Product at Continuum Managed Services.

RT: And what does that mean, exactly?

FH: I'm responsible for both our product and server strategies, delivering solutions to Managed Service Providers. I spend a lot of time with them, trying to understand their challenges and needs. I try to find opportunities to make our current solutions better, trying

to grow our businesses from our technology and software standpoint but also how we can plug in our service component into the overall main and service challenge.

RT: I've had a couple of people speak to me, and they view Continuum as a service company as opposed to a product company. How would you address that, being the Vice President of Product?

FH: It's a great point, and maybe a common misconception in the market. I guess, ultimately, it's in our name (Continuum Managed Services), but that's because we service Managed Service Providers.

To give you a bit of context, we have over 250 R&D (research and development) engineers, that are writing software that MSPs are interacting with every single day. Quite often, our differentiation tends to be on the axis of service, so helping MSPs reduce expense by using offshore capabilities and things like that.

We have a wealth of software and software developers that truly drive a lot of the automation and the day to day interactions that MSPs have with our tools.

RT: What does a typical day look like for you?

FH: I'm usually in the office by 7am, as I get my quiet time then. I spend a lot of time in planning meetings, planning from both a research and development standpoint, from getting market problems right, then also planning how we enable sales and marketing teams, so I have that full spectrum.

Then, I usually try to have a couple of partner interactions during the week, to make sure that the things we're thinking about are grounded, and having people challenge us on what we think we've learned, to continue to refine that learning.

RT: I want to get to your keynote presentation shortly, but before we do, something that Michael said during his keynote about the market being dominated by the top 20% and lots of consolidations and mergers and acquisitions within the field.

That brings an interesting situation where during mergers different MSPs would use different sector tools and they need to come together. How could Continuum help them with that scenario, where they've got multiple tools and they need to consolidate into one company?

FH: I think first and foremost we can help them consolidate on our tools, most importantly. There's definitely consolidation going on in the market, and it is something that we think about. Part of our platform is tools that help people very quickly (in a matter of days) migrate hundreds or even thousands of endpoints from one RMM to Continuum's RMM.

If someone has a pre-existing backup and disaster recovery application that they're using, we can migrate legacy snapshot images from different providers and translate them into our formats. We can virtualise even their legacy data as well. We've looked at the legacy data problem in general as we grow our business, and I think it does begin to play into the consolidation too.

We need to be chosen as the ‘tool of choice’, which means hopefully we’re delivering the most value when MSPs come together, but we are thinking a lot about how to help people make that transition. It’s key for consolidation, but it’s also key for us day to day running businesses. There’s not many MSPs without an RMM tool today, but we’re adding more every day. We need to always be thinking about this.

RT: I think I’m seeing Continuum move towards being a business platform for MSPs more than anything. I guess first of all, would you agree with that? And if you do, how do you think that changes the way you view your products as a platform as opposed to tools that MSPs use?

FH: More and more we’re bringing together the tools that we have and trying to make them an integrated service delivery platform. That is something that I think is really important, because if you step away for a minute from our point of view, think about the client served by the MSP.

All they care about is, ‘Is my IT up and running? Is it secure?’ and more and more they actually really care, because they understand that, as small businesses, they’re the prime target now, not just an accidental target.

And third, ‘Am I meeting different compliance standards that are relevant based on my geography or my industry?’ If you think of that, there are a lot of different things that go into meeting those client needs.

Traditionally, we’ve had RMM, we’ve had BDR (back-up disaster recovery), we’ve had security. Those are point solutions in some ways to solving them. So, what we’re trying to do is integrate them to bring together our tools and point solutions in a different way, so there’s a connective tissue between them, and ultimately making it so that security is aware and understands when the last backup was.

Or if there’s a security event, understanding that the last good backup was actually three weeks ago, because that ransomware or whatever has been sitting there for a while, so restore there.

Or, that an RMM understands that we have an issue with respect of vulnerabilities on a security front and does auto-remediation of those things for our partners. The more that we can take information from what was traditionally a one-technology silo and apply it across the problem, the more we have an integrated business platform for MSPs to solve that problem the client cares about: ‘Keeping me up and running, keeping me secure and helping me meet my compliance needs.’

RT: I want to delve a bit more into a couple of things you’ve said there about compliance and what the end user wants. We also need to delve into the security situation.

Continuum are known very well for what we would traditionally call a NOC (network operations centre), more often known as the master MSP model. You’ve got SOC coming

along (security operations centre) – for people who aren't familiar with what a SOC is, how would you summarise it?

FH: A SOC is pretty simple and it's analogous to a NOC, with a different skillset. Ultimately, a SOC, for us, is a centre or war room of trained security experts that are monitoring our tools, our MSPs and MSP clients' environments for suspicious activity, using tools, technology and knowledge to determine what suspicious activity is malicious. And when malicious, mitigating and then remediating that activity, with a cybersecurity lens.

What's great about our model is that we can have some remediation done by NOC, we can extend things out, but it's really security expertise. The reason that's so important is that enterprises today are really struggling to hire security expertise. MSPs have really struggled to hire, because they're competing against the enterprises.

We have so many partners that have trained their own staff to be security experts only for them to go and get a job making twice as much money at a large enterprise. By having that SOC and that differentiation in and around our tools, it's going to be very powerful for MSPs, much like the NOC model.

RT: I got a sneak peek of the SOC dashboard earlier on, which as a geek I really geeked out about.

FH: It's pretty cool stuff, actually. It's cool to see the tools they use, although I'm not going to pretend I understand all it does in that active threat world, but it's pretty powerful.

RT: Going back to something you said about meeting the end users' needs: You're a US-based company but you've got a global reach. How do you tackle local compliance requirements, and of course there are many different regions across the world with different compliance requirements?

FH: It all starts for us with expertise. GDPR is one of the biggest things that's been talked about in Europe, so the first step for us was making sure that our solutions were certified for GDPR and we were handling personal information correctly per the standard.

That's a great example and it was a real eye-opener. It's really more of a people and process problem than even a cybersecurity problem, frankly. It all starts with understanding, and that's a recent example.

We've done some work in HIPAA in the United States, which is the Health Care Regulatory standard. We brought in experts, and we worked with them in order to develop explicit measurements, monitoring and reporting in and around the status of an environment for HIPAA compliance.

We'll be doing more and more of that for the compliance regimes that make the most sense. Part of one of our steps is to really dig in with our team in Europe and look at what are the more common compliance requirements that have security components to them.

GDPR has all the noise and news, if you will, but it's more about personal information than exactly cybersecurity, where there's other local regimes that are more relevant to our MSPs' clients in Europe.

RT: To that point about the globalisation of IT – services like Microsoft Azure and other cloud services are becoming increasingly a standard part of what the MSP does day to day. How are you adapting to these requirements from MSPs to work with those platforms?

FH: Traditionally, much of what we've done has been monitoring and managing on-premise technology for MSPs, because that's still the majority of the workload. About 8% of SMB infrastructure is moving from on-premise to either the public or private cloud a year. It's still moving slowly overall, and that's accelerated quite a lot to even get to the 8%, but I want to be as agnostic as possible to where the workload is and to deliver value to the MSP in managing that environment.

We're really looking at what are the problems that are unique and different for the cloud? First of all, our RMM agents actually work in Microsoft Azure for example, or AWS, monitoring servers, and about 10% of those are in the public cloud.
One of the things we have announced today was that we're greatly extending our Azure monitoring capability to monitor out of the box about 10 Azure services, not just the servers. This is so we can look for if they're available, are there problems restarting them, cloning them, having our NOC work on issues for the MSP.

We've also announced that we're going to be able to back up servers that are in Azure using our Continuum BDR product as well. We're looking at industry problems and putting solutions forward to them.

On the security front, we've actually done something interesting. Office 365 is the most highly-adopted SMB application with respect to SaaS (software as a service). Over 50% of SMB's are on Office 365.

As we look at our traditional lens, Office 365 doesn't really have a monitoring and management problem, because Microsoft has done a really good job there, but it's one of the largest attack vectors for cybersecurity.

Understanding the market and the SMB, what we did was dug in and said: 'Our first solution for Office 365 need to be in and around the monitoring of the security posture using our Profile and Protect offering, and then active threat management using our Detect and Respond offering.'

This is looking for multiple failed logins, logins from known bad IPs or odd geo-locations where a person usually isn't. This gets about the user not the endpoint, because it's SaaS.

That's a great example of extending to the cloud with our platform but focusing on the biggest problem, not necessarily one that we would have traditionally focused on three years when we were just thinking as RMM vendors. This is all part of our evolution.

RT: You mentioned a word earlier on – agnostic – and we also talked about mergers and acquisitions. We're also seeing a lot of mergers and acquisitions in the MSP vendor space as well. How would you say that's affecting your strategy towards API (application programming interface) and integrations in allowing other vendors' products and tools to integrate?

FH: It's a great question. The more technology markets consolidate, particularly in the mid-market SMB-type space, the more there's a demand for vendor cooperation and openness. The most successful companies in this type of segment have an open philosophy to things.

We're working to greatly extend the APIs that are available on our platforms so we can do partnerships and work with other vendors, even 'co-op-ertition' if you will. That will also allow our MSPs to do integrations to things as well.

I think openness is going to win in this market like it has, frankly, in so many markets, because the days of traditional vendor log-in and closed segments, even at the enterprise level, is getting a great amount of pushback.

Markets demand openness and they don't want to be forced into things, and I think that's going to be our philosophy. We always hope our tools are better, so we have to make them better. The client, the MSP, wins when people are open.

RT: Talking about the MSP winning, you've got an in-house UX (user experience) team. How do they ensure that the UI (the user interface) that the MSP engineers see is the interface they actually want?

FH: I'd love to say it's more art, but it's all science. We do have a team of UX engineers, and first we begin with a problem that we're trying to solve. They'll then interview several of our partners – we usually try to get five to 10 in the early days. They conceptualise the problem and the workflow a little bit, and you do mock-ups.

From the mock-ups you don't go to development, you go back to those partners and a couple of different partners, and you iterate a little bit to start solving the problem. Unfortunately, you can't show it to everyone, you need to get it right for the most part.

Then we start writing real code and we get it back in front of partners before we ever get to production and we iterate that process. We try to do it quickly and use Azure development like every vendor, but that UX team is so key, because what we want is to delight our users when they're using our software.

Some of the gains we made in the last year and will continue to make into the next year are all about simplifying the user experience, making it super-intuitive and making it workflow-focused, so when a technician's going in and solving a problem, it's clear, simple and easy for them to achieve that task or outcome they're focused on.

RT: Let's talk a little more about that workflow focus. You've announced some big modernisation for the platform, including a focus on automation. Tell me more about that as

well – what can you do to help the engineers not have to do things and stuff just happens for them.

FH: I think there's several things. One of the biggest things Continuum has always done is we've had a concept of what we call Telemond – and Telemond is looking at all the alerts and conditions that come off any type of machine, performing some correlation and identifying what the real challenge is, or if there is a real problem.

We've extended those capabilities also to desktops, not just servers, and that's been important. From there, when something's identified as a true, Continuum alert, after we get the noise out, we are actually able to take a type and have a technician automate the running of a series of a script or scripts using our task and sequence capability.

We can auto-connect condition happens and run this. We're doing a lot of that, and how we think about things is to take the condition out of the box so you can have the full automation. We have hundreds of out of box scripts, and what we've also done is expanded scripting to release this concept of sequences so that we can run a series of scripts in a serial event.

Based on the outcome of any given script, we can choose to run a different script – think of it like conditional logic. That's hugely powerful for automation and really will make technicians significantly more productive.

RT: As a former technician myself, I'm really excited about that! Anything that makes life easier is great.

Michael George

RT: We had great feedback on the last episode we did. You're a busy man here at Continuum Navigate – you've got 700+ MSPs here. What's been your top goal for Navigate this year?

MG: The industry right now is at a very important crossroads that it needs to be paying attention to, and we want to make sure our partners are as prepared as possible to meet the challenges ahead.

When I say 'ahead', I mean at their feet, not way far out. The big issue is that small medium business market has largely not been under attack from cybercrime, and as you know, large enterprises have been for a long time, as have government systems.

As those industries have spent billions of dollars getting all those systems locked down, they've made slightly more difficult for cybercrime, and it's turned its attention to the small business market, which has spent virtually the last 20 years getting interconnected and hyperconnected and not paid a lot of attention to security.

With a fairly easy initially, but then over time some technologies which have made cybercrime a much more pervasive part of the small business market, and somewhat

random, both simple and sophisticated techniques are being used to attack small businesses.

They have figured out how to exploit them with ransomware, to steal data, lock down or shut down systems and other things that will impair a business' ability to continue.

Now that that's upon us, unfortunately, most customers are now in a frantic frenzy of, 'Am I going to get attacked? Am I protected? I have security on my invoice, I'm paying for it, so I must be secure in some way.'

The MSP market in general, and very broadly, is really flat-footed when it comes to addressing these issues, because the security that they have been providing has been appropriate at its time (malware, AV and rudimentary endpoint protection elements) but with the level of sophistication there is, the need now is for isolation and remediation. It's an imperative.

It's a very challenging dynamic, where the MSP is not prepared to address this pandemic issue.

RT: I want to talk lots about security, but something I want to touch on first, from your keynote presentation – you mentioned the big changes in the industry that you see, such as the Pareto Principle: 80% of the revenue being driven by 20% of the MSPs. How is that separation coming about?

MG: We've both been doing this for a while. All of these macro market trends end up evolving this way, so this is not a unique phenomenon, so much so that there is a broad principle that's well understood and applies to most of the way these markets shake out. That one's upon us now and it's absolutely right. They say that today in North America there's about 40,000 MSPs by SIC code. If you look in the UK and throughout the pan-European markets there's also about 35,000 or 40,000 MSPs in that geography, and it's all highly fragmented. There's no concentration.

There might be some larger providers but there are very few. Most are of the cottage industry that has been the backbone of the MSP market since its genesis and that slope of separation to the 80/20 rule is going to happen very quickly, as it usually it does.

It takes a catalyst, something that takes a market or industry from a tipping point or place of critical mass and absolutely transforms it very quickly. The catalyst in this case is security, and cybersecurity in particular, and the need for more secure capabilities by the MSP to protect their customers.

That's the macro-dynamic, and very clearly over the next two to three years the market is going to take shape. The shape it will take, and the type of companies involved will be those who are well-prepared and well-equipped and deliberate about executing on the needs of the market. They're going to become part of that 20% and dominate 80% of the revenue.

They'll have a lot of sales DNA inside the organisation, they'll be very clear about gaining market share and not just trying to cross-sell and upsell their existing customers, but going

out and getting new customers. They'll have a comprehensive suite of products and services that enable them to do everything from what a traditional MSP used to do in combination with what a new managed security service provider needs to do.

I don't think that those two things will be different any more, I think that they will be one and the same, and that will be the catalyst for the separation and the separation will take place over the next two to three years.

RT: I want to pick up on some more stuff from the keynote, but before I do, I think it's three or four times I've seen you present now, and you're such an engaging presenter. Do you get nerves before you go up in front of a big audience like that?

One of the perks I get from doing this podcast is I get free consultancy from brilliant people. I get very nervous in front of big audiences and you seem so smooth and engaging – how did you get trained up on being a great speaker?

MG: First of all, you're very kind to say that. In terms of being engaging, I think the content speaks for itself. We spend a lot of time and do a lot of research, and the material I'm sharing in those keynotes are things that we believe are really important things for the market to understand.

It looks easy because it is easy, only because I'm very passionate about what we do and the role we're playing in the entire MSP eco-system, and so it's not difficult for me to express that passion. Just look at the content and the analytical and thoughtfully-organised material, which I'm not taking credit for, as we have a spectacular team that do the analysis and research.
We have financing by Thoma Bravo, who own more than 90% of the technology providers that are serving the managed services market, and they know a whole lot. They research macro trends and dynamics, and they understand who the winners and losers are going to be. That's why they bet billions of dollars on them, and they're usually, if not always, right.

They share with us a lot of that analysis, and it's been a privilege, frankly, to be the mouthpiece for both a tremendous amount of statistical analysis and also a fantastic marketing team and the team in our organisation that help us organise it in a way to be able to share it with others.

RT: Back to your keynote, and there was a fantastic quote you shared here, which I'm going to repeat back: "BDR is to security what sprinklers are to fire prevention." I love that – can you elaborate on that a little for us?

MG: BDR has got an incredibly important role in the IT services ecosystem, so I don't want to diminish its value, but there are some vendors out there who call it data protection, and in turn MSPs call it data protection, and they've been selling it to their customers that way, without the clarification of saying, 'It's really an insurance policy, but it's not a security tool.'

That would have been an important distinction to make, and since it hadn't been made, there is a false sense of security on behalf of those who went out and licenced a BDR from their MSP with the sense that, 'Well, my data's protected', and that sounds proactive and pre-

emptive when it's not. It is reactive, and much like a sprinkler system only goes off when a fire's ablaze, and there's already fire and smoke damage, it also causes water damage.

If you really unpack the way a BDR works, oftentimes people are trying to do a backup when it's already too late. Bots, as we know, infiltrate networks and systems, and sleeper bots sit for 21 days on average, and in the meantime, they've done a lot of damage. Backups are continuously backing up and bringing that malicious software into the backup environment.

It's creating a false sense of security, and it's creating a challenge, frankly. We're hearing from a lot of MSPs who are mis-positioning it that way, of coming in and saying, 'I'm really having a hard time finding the right kind of security solution to my customer in the security space, because when I sold them a BDR I sold it positioned this way, and now I have to explain that it's not quite true data protection, it's in a sense an insurance policy for when I fail at security.

'It doesn't necessarily mean that I'm going to be able to prevent a security incident and remediate it out of the network. I'm allowing it to co-exist in your environment and I'm using this to go and find a recovery point that we believe is prior to the malicious attack, and we didn't have time to inoculate the rest of the system. It's spread and so we've backed up a number of spread, malicious pieces of software into the system so I've got to go way back.'

The problem there is that's productivity loss. Now we're having to wind back pretty far, because this problem sat undetected and un-remediated and so backup systems are not a problem unless they've been mispositioned as a security solution when they're not.

They *are* a part of the security equation, and I don't want to misrepresent that, and ours is a critical part of it too, but we're doing some things to provide very early detection of some anomalous activity, and as soon as we do that we'll provide a signal alert through our system to notify our BDR to back up everything on the network except for that one device where we detected some anomalous activity.

That way, I'm cleaning up when I'm capturing everything else, but I'm not backing up that malicious piece of software. That's just one example of how you can better tie in true BDR to a true, holistic, cybernetically-connected system that will really address the security issue in a much more comprehensive and real-time way.

RT: I'm a bit of a history buff when it comes to the history of IT. You talked about something during your keynote, a connection that I'd never made before, to do with digital Darwinism, to coin a term.

You talked about Xerox and how they've lost $100bn from their pricing since 1999, and you also gave the example versus Sharp, one of their competitors, and how they've risen during that time. I thought it was a fascinating story, so talk a little bit more about why you see Xerox has fallen and Sharp has risen during that time – what happened there?

MG: That's just one example, but very illustrative of this concept of digital Darwinism and the rate of change in and around the digital world we live in today, and how it happens very

quickly. Companies have to evolve, adapt and change, and I use the term ‘pivot’ from one transformational change to the next in order to not only survive but to be successful.

The example of Xerox and Sharp was to illustrate a clean example of two companies that both rose around the same fundamental digital transformation, that was in the days of facsimile. Both of them were leaders in their respective categories – Sharp in the small business market and Xerox in the enterprise market.

From essentially the mid-80s on through, their revenues and business platform rose, because they went from what was simply a copier to what became a multifunction device. That second principle function was facsimile, and these are two companies that grew and benefited tremendously from that evolution.

The example was clear: Xerox being the leader in the enterprise space ended up becoming a great company of innovation. They invested a lot and created a thing called Xerox PARC, which stood for Palo Alto Research Center, and it was there that they had invented some very important elements of the personal computing transformation.

They invented the GUI (pronounced ‘gooey’ - graphical user interface) and the mouse. Of course, we credit companies like Apple and Microsoft with that, because they were the ones that actually did something with it, and pivoted and transformed their ideas into the personal computing era. Xerox was a company that failed to even appreciate what they had and what they had invented. They did not grasp that technological transformation and they did not pivot quickly enough.

As you know, as a history buff of IT and technology as you are, the personal computer, in combination with the internet, and now with docu-sign and the other transport mechanisms using the hyper-speed of the internet and the clarity and perfection of a document (not the reproduction of one) really became the cause of the demise of the use of facsimile.

At its peak, there were 100m facsimile machines produced, with Sharp and Xerox being two of the largest producers of it, and 17bn documents transferred around the world by a facsimile. The demise of that was really the cause of the demise of the very thing that Xerox invented and they just didn’t grasp it. They didn’t make the pivot and went from $110bn at their peak in January 1999 to today, where they’re trading at $6.5bn.

They’ve lost over $100bn dollars of value in that time, and it’s just astronomical. It’s not a good story, but it’s a story that everyone needs to understand. The elements of that transformation and why companies like Sharp, who’ve figured out how to pivot and embrace the next transformation had a race to the future rather than resting on the laurels of their momentary success have done well.

The rate of change in technology is hyper-speed compared to the industrial revolution. The digital revolution is taking place at astronomical rates, so the need to move quickly is an imperative. Xerox failed to do so and it’s a sad story. Sharp was one of the few companies in the same fundamental category (technology provider of office equipment) pivoted and pivoted, and today they are one of our largest partners.

They're using our platform to go to market in remote monitoring, backup, security and all the other elements that we make available, so we're very pleased to be with a true adopter of innovation and a company that knows the race to the future.

RT: You've got plenty of other people you need to see today, but I can't let you go without asking one other question about IT history. Is it true that you own an original Pacman console at your house?

MG: Something of your own personal passion I understand?

RT: Absolutely, yes. Retro gaming is a big thing for me.

MG: It is, in fact, true. I also talked in my keynote about how timing is everything, and one of the things I was very fortunate about is that when I was in high school my job was buying old pinball machines, the old, physical, mechanical pinball machines.

It was a lot of fun, and I had a high inclination to electro-mechanical design, telemetry systems and other things. I was very oriented to that, and I used to buy these old machines for $25 and $50, load up my parents' garage and spend nine months of the year fixing them up and repairing them. Not just cleaning them, but fixing the solenoids and all the different elements to them.

As we approached the holidays, I would advertise them in the local classified 'want' ads, and that was my way of making a living through my high school era, and then when I was heading into college, again had good fortune, as the saying goes: "Fortune oftentimes is stumbling from one failure to the next without the loss of enthusiasm".

The next thing I stumbled into was the same distributor made available to me the Pong games out at the time, so I turned my attention to that and started a video arcade business while I was in college. We went from one little pizza parlour around the corner to owning seven arcades in one state and in another state, we were the largest supplier in a tourist community of all the games in the bars and restaurants.

Shortly after, Time Magazine ran an article equating owning a video game arcade to owning a pot of gold, and that was my signal to sell the business. We also had the good fortune to be able to do that around the time I was graduating from college, so it all happened very quickly.

When we were approaching the end and I was selling the business, the Pacman machine was the last one I bought. The games got more sophisticated, such as Defender and Tank and using raster scan technology and all of kinds of terrific innovations, but this was the machine I bought, stored and kept with me, knowing one day I'd have children of my own who would enjoy both the history and the fun of it.

We have a little game room in our home and my three teenagers play it with the same level of fascination and enthusiasm as perhaps you and I might have when we were that age.

Thank you for asking about it, and I hope the story wasn't too boring for you!

RT: I think we could record an entire podcast just talking about your history with video games. Maybe I can twist your arm to get a photo of that Pacman machine!

Michael, I know you've got to rush, so thank you so much for taking the time to spend with me today. I really appreciate it, and congratulations on another great Navigate Conference.

MG: You're very kind to say that, and thank you for your support and all that you do for the community. Having built an MSP of your own, and a successful one at that, I can't think of a better voice to channel the needs that the MSP has today, and the right kinds of editorial skills, as well as the way you approach a story and the interest to this. It's a very important way for MSPs to learn and to grow and to benefit. Thank you for all you do for the industry as well.

RT: Thank you – that means a lot to me.