PARTNER PERSONIFIED

Paul Ponzeka is CTO at Abacus Group. We talked to him about why providing great customer service is more important than offering the latest technology, and the biggest security threats that are facing the financial services sector.

By Orbit TRC

Which is more important: great customer service or the latest technology products?

At Abacus, we pride ourselves on delivering great customer service. Besides our proprietary client portal, we don't create much of the technology we use ourselves so the difference in what we do is how we deliver great service to our customers in such a high-touch industry.

Customer service has always been paramount for us. One of the things that we always say is the ordering the pizza question: someone's at a hotel; they call up reception; they're angry; their Wi-Fi isn't working; they're trying to order a pizza. For us, great service is: okay, let's order you the pizza and then we can look at fixing your Wi-Fi. It's about being attentive and trying to listen to the users and resolving their issues, and doing things that are more important than simply having the latest product.

I think having the latest technology is important but I think offering good service is more important. If we have the latest and greatest shiny penny but no one wants to use it because it either doesn't work or it doesn't solve a business need, it's a waste. But if someone knows that their computer always works or that we're there to help them fix it, building that relationship and developing that trust with them is a lot more important to us than just the technology.

What role does automation play at Abacus, for employees and customers? What benefits does it bring?

Automation has been an area of huge investment at Abacus over the last several years. The groups that have been the primary driver of that are our DevOps and software development teams. We've used these automation efforts to drive repeatable process and provisioning for our customers.

It was a multifaceted endeavour for us. First was automating some of the baseline tasks within the organisation. We asked ourselves how do we make ourselves more efficient and it was a simple thing like let's make our workforce 'smarter.' The easy way to do that was to take the bottom 10% of their tasks – the repeatable stuff – and automate them. The other thing was we saw that we needed to start providing more visibility and transparency into some of the infrastructure to our clients and doing that through automation and software investment was the way to go for us to be able to report on what we were doing. Instead of having to hire five new people to do the same exact tasks, but just more of it, let's hire two or three people to do that and allow the really smart engineers to focus on new areas of improvement and development.

So not only has it helped to scale that part of the business but it's also allowed us to continue to push the envelope on R&D and shorten our time to market on new product releases.

Abacus offers a public cloud based platform. Why did you opt for that rather than a private cloud based one? How do you think the cloud will develop in the future and which version of it do you think will win out?

We were originally in the private cloud but we built our public cloud platform because the technology stack provides immense opportunities for our clients to compute in a modern way. I no longer just have a corporate device in the office – I now have a corporate device in the office, I have a laptop at home, I have a mobile device on the go. I'm in the car, I'm on the train, I'm at the airport, I'm at a vendor site – I need to be able to work. I think people were saying, 'I want to be able to work wherever I am with the same workflow that I would have in the office.' I think that's more of the modern way versus the previous way of, 'how do I either physically or virtually get back to the office to be able to work?'

The more modern way is bringing that compute to people wherever they are and I think one of the biggest boons of public cloud is that ability to work flexibly wherever you are, without a loss of the fidelity that clients were clamoring for.

Abacus Group has invested heavily in automation

The public cloud allows Abacus customers to compute in a modern way - whenever and wherever they need to

The public cloud allows greater visibility for security teams and compliance teams on the customer's side, and dramatically reduced our time-to-market efforts. We think that, in the future, there'll be an increasingly heavy shift to the public cloud, but ultimately it will become a hybrid approach.

Cybersecurity is a hot topic, with the recent spike in ransomware attacks. Can you share your thoughts on the current situation with us?

It's active warfare, essentially, at this point!

I think the biggest thing I've seen in the last three or four years has been the shifts from having a conversation about usability versus security to usability no longer being a valid reason for not adopting certain cyber security protocols.

So we've seen that our role at Abacus Group has become much more in the forefront than it was previously – we're taking a more forceful approach with customers and saying, 'We're not going to allow you to make some of these poor decisions that maybe you're just not as educated on,' and really pushing the cyber security landscape forward.

So we're doing things like requiring multifactor passwords, really pushing patching, no longer allowing bad cyber security practice to stay and the client to sign off on it.

I think the big shift over the last three or four years is, whether they want to or not, dragging customers along. But they are also getting pressure from regulatory bodies and the investors, who are becoming much more educated on it and are pushing them to do it as well. So I think you'll continue to see that movement forward.

How have Abacus' discussions with fund managers about technology developed over the last decade? What are fund managers' concerns and needs now, and how do you see those changing over the next ten years?

We've seen fund managers' awareness around cybersecurity be the biggest area of change in the space over the last several years. Where previously they would come to us and ask us what to do, they are now much more involved and educated on the needs of the business.

This has allowed the industry in general to jump ahead as now we are designing cybersecurity solutions around an organization's security business needs instead of trying to drive it from the technology side.

So we're seeing that firms are now coming with the proper sponsorship from the business team on their side to say, 'Hey, we support a better cyber security stance now. What can you do to support policies that we want to put in place?'

I think that when you have that high level sponsorship, it has a much better chance of success in permeating through the organization.

What unique needs do alternative investment firms have when it comes to technology, and how have they developed over time? How do you think they'll continue to develop in the future?

I think that alternative investment firms are unique in their relatively small size of headcount compared to their enterprise needs regarding cybersecurity – the amount of computing or technology needs that they have versus how intensely they use computing platforms rivals some of the most demanding

enterprise organizations.

A lot of times, because they're small, they lack that upper management business sponsor who's the CTO or CIO and a decent support staff behind them who is able to translate the business needs and goals into technology. So you have someone like a CFO or CEO who is that business sponsor but doesn't have a background in technology, so they have a lot of needs but they either have difficulty communicating them or finding someone who can oversee it.

I think the space will continue to lean on third parties like Abacus to provide some of that direction.

What demands are regulators and investors making that Abacus' products enable alternative investment firms to meet? How do you see those demands changing in the future? And how will technology have to change to keep pace with them?

The demands will always be changing and we will continue to adapt our platform as needed.

Things like the OCIE alerts regarding how firms manage inventory and software versioning are all maintained by our Abacus platform. Advanced next-generation EDR endpoint solutions to manage cyber risk, all encased with our managed SIEM solution, provide the requirements of firms to not only meet regulatory requirements, but also investor requirements as well.

What are the biggest security issues facing financial services firms at the moment and how can they be addressed?

I think ransomware is always going to be there but the biggest one that we're starting to see is very targeted spear phishing attacks, where people are going after these firms, are doing their homework, they're researching the organizational structure, and attacking process weakness in these firms. These firms are smaller but they deal with immense amounts of capital, and sometimes they lack the proper processes and procedures to protect against these security weaknesses, and the hackers have gotten keen to that.

So I think phishing has been the biggest one that we've seen where people are going after the CFO or the CEO, requesting wire transfers, things like that. Coupled with a little bit of the small-business-style feel that some of these firms still maintain, those become problems.

Targeted phishing attacks are tough because they target the users, who are always the weakest point. When an employee has people calling them on the phone, saying, 'hey, I'm John from XY&Z, can you transfer some money,' it's only user education that will stop it. So it's really difficult to stay ahead of that, especially when these firms are dealing with such small teams.

And the fact that so many people are working from home as a result of the Covid-19 pandemic makes them even more vulnerable to spear phishing attacks. If you're a chief accountant and you're handling transfers and you get an email from your CEO telling you to send one, if he's in the office it's easy to speak to him about whether you should send it.

Also, at home there are bigger chances for distraction or doing multiple things at the same time, and someone just not thinking about it and saying, 'Okay let me just get this done,' and not paying attention to some of the other warning signs.

The other thing we've seen is that as people have worked remotely, the frontline of the corporate entity has moved to the home: someone's working at home when their son or their daughter is online doing something they shouldn't, their PC gets infected, and now all of a sudden the corporate entity is under attack.

The reality is that the corporate surface area is much broader, resources are stretched, and all of that combines to make it a lot easier for these things to pop up.

Abacus is helping customers to secure themselves againt cyber attacks