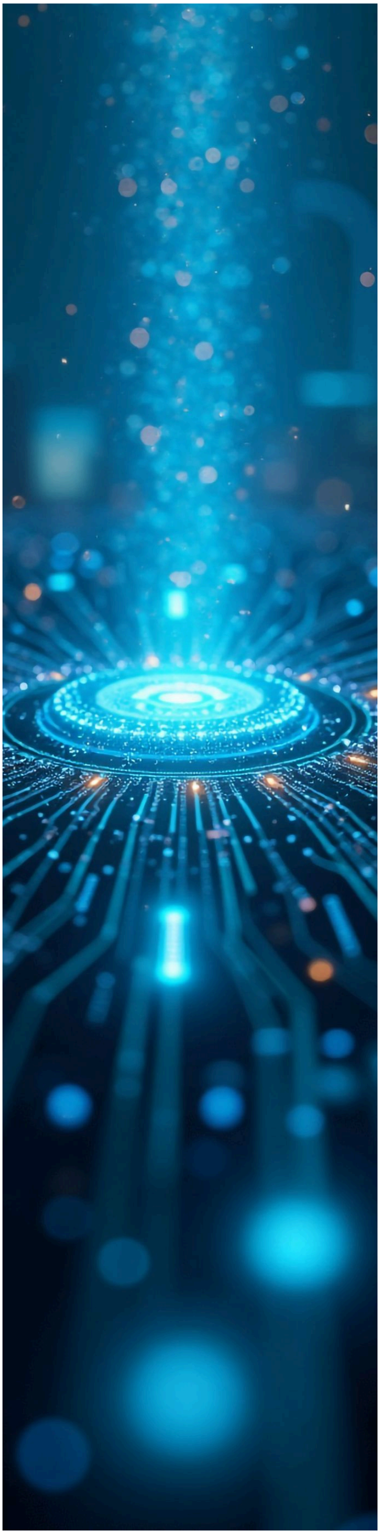
Linedata

Future-Ready Portfolios: Exploring Technology as a Lever for Value Creation



Private equity has seen a shift from traditional financial models to a more asset-focused approach. Central to this shift is the role of technology, which serves both as a driver of value creation and a point of vulnerability, particularly in terms of cybersecurity and technological disruption. Our panel explores these themes, in particular how technology impacts asset quality and value creation in private equity.

SPEAKERS

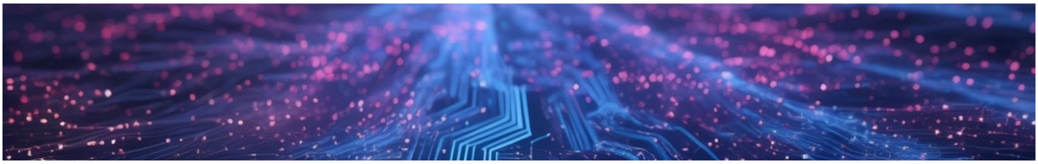
Josh Barber
Director - Cloud Services and Support,
Linedata

Gary Marshall
Director of Technology,
Paine Schwartz Partners

Bill McSorley
President,
WM3 Group LLC

MODERATOR

Aftab Bose
Head of Private Markets Content,
Private Equity Wire



Aftab Bose: Let's start by discussing how public cloud technology and cybersecurity help create value at the asset level in private equity. What red and green flags should investment firms look for during due diligence?

Gary Marshall: For me, the biggest question during tech diligence is whether the acquisition target is aware of or appreciates its technology stack. Many of these organizations are just trying to get through the day and aren't paying sufficient attention to their tech stack, infrastructure, and cybersecurity. So, we go from there.

Aftab: Does your due diligence cover both digital infrastructure and cybersecurity? Are firms typically aware of all cyber risks?

Gary Marshall: Historically, cyber was mostly ignored in private equity. Recently, it's become more prevalent in the news, people have heard about large data leaks, hacks, etc., so it's entering the common conversation, and people are paying much more attention to it.

Aftab: How have you adapted your due diligence process to fully address tech stack risks?

Gary: It depends on the organization. I don't think there's a one-size-fits-all approach. We have a technology DDQ, but ultimately, it involves looking for inequities in individual organizational systems and moving from there.

One thing I hone in on is their cybersecurity awareness. Are they doing cybersecurity awareness training? Do they appreciate how their remote access systems are secured? If you are going to acquire one of these organizations, you're bringing all that tech debt along with it, so that's what you're trying to hedge against.

Aftab: All right, fantastic. Bill, is that your experience as well?

Bill McSorley: Yes, it is. When I'm brought into the acquisition process, one of the first things I do is ask for the target's documentation. Do they have a DR policy and incident response plan? Oftentimes there are no written policies around anything. That is a red flag of, "Okay, how seriously do they take cybersecurity?"

A lot of times I'll run my own vulnerability scans against their external assets. They'll give you a report, but it's sort of a 'trust but verify' thing. I want to see for myself with my own tools what I'm dealing with. Have they patched in a year? Also, if there's a big churn with their technical staff, that's a red flag to me. And then the obvious, "Tell me about your breach history." That's always an awkward conversation, but it's important.

> "For me, the biggest question during tech diligence is whether the acquisition target is aware of or appreciates its technology stack. Many of these organizations are just trying to get through the day and aren't paying sufficient attention to their tech stack, infrastructure, and cybersecurity."
> **Gary Marshall**

Gary made a great point that people are becoming much more aware of cybersecurity risks because they're reading about it every day in the paper. You don't want to be on the cover of the *Times*, right? So, there's much more awareness of the seriousness of it, and it goes right up to the Board level. That's a contrast to 10 years ago when it was a check-the-box sort of thing.

Aftab: How do you help firms plan for longer-term cyber threats and how they might evolve in the future based on the business model and infrastructure?

Bill: A priority for me is third-party risk. We're all aware of supply chain attacks that have gotten a great deal of coverage. Solar Winds comes to mind. Excellent company. But when it got hit with a supply chain attack, it caused a lot of problems. So, I'm not just doing diligence on the target, I'm also putting it on their key vendors. It gets complicated, but you really want to know that it's buttoned up and they're paying attention to it.

> "You need to be aware of your costs and know how to architect and tune [public cloud] properly so you're not spending an unneeded fortune every month."
> **Bill McSorley**

Aftab: Josh, how do you guide clients in terms of conducting due diligence, considering the red flags, resources, and various other factors involved?

Josh Barber: You tend to pull the thread of a problem, find further problems, and keep pulling the thread until you hopefully get most of them. Anecdotally, we did an assessment recently of a portfolio company, and they were still running Windows Server 2008. Now, their head of technology was very, very well-educated and knew what he was doing. He was desperate to get rid of it. But when you find something like that and you start pulling the thread, it often turns out there are a lot more demons and a lot more nasty things to find.

So, we'll pull a thread and say, 'There's this problem, and this is how we would mitigate it, for example with public cloud.' You can buy extra time with Server 2008 in Azure, as an example. Not that anyone is recommending you continue running Server 2008 – I will make that crystal clear – but with Azure or Amazon, you're very, very scalable very, very quickly. You have much better protection than you do on your on-premise server.

One thing I do with one of my PE firms is meet regularly with the deal team. They get how important all this stuff is, right? It's mundane, and sometimes it's in the background, and they're excited to get the deal done, but I've educated them that uncovering things now will save them a lot of headaches down the road.

Aftab: Beyond addressing current problems, how do you advise clients to plan for potential future threats and evolving risks, especially when scaling up?

Josh: A lot of it's going to be public cloud moves because that is the going to be the *de* facto future, in my opinion. It brings all the benefits that private hosting doesn't have. With private hosting, I can't add compute quickly; I can't add disks quickly, so there are lots of advantages to public cloud. We can do it quickly and fairly seamlessly using tools like Azure Migrate.

So, no matter how much bad news there is, we can always come up with a good news plan. It's just having to get all the bad news out. We're not trying to pan anyone or attack anyone.

I just want to know all the skeletons in the closet so I can say "This is how we're going to fix them, or this is what we recommend." It's easier to be upfront and blunt so we can get all the red flags to green.

Gary: That's a very, very good point. Being able to have those conversations requires a certain amount of trust, but once you have that established, that transparency is absolutely paramount.

Aftab: Do you see public cloud as the future? If yes, why? If not, why not?

Bill: Yes, I absolutely see lots of workloads, if not the vast majority of them moving to public cloud. Microsoft and Amazon and Google have spent a lot of money and time and resources making sure it is secure. The capabilities and the benefits of moving to public cloud are vast. The OpEx versus CapEx model reduces your total cost of ownership. Cloud providers can secure their data centers much better than a company can.

Also, the explosion of using machine learning, AI, and data analytics with your data – you're not going to build out systems like that on-prem. You're going to do it in the public cloud. So that's a huge advantage, especially for any company that's getting wise to analytics.

> “Make sure your user base is trained. If they get an email out of the blue saying, ‘Oh, we need to close this deal immediately, text me this to this cell phone number; I’ve lost my other cell phone,’ there need to be enough red flags going in their head so that they don’t blindly follow it.”
> **Josh Barber**

Aftab: Gary, what are your thoughts on that?

Gary: Bill made a lot of very, very good points. I will say that some of the happiest days of my life were the days that my sons were born and the day that we got off Exchange on-prem! Some things are potentially better suited to you running them yourself, but the transition to an OpEx model rather than a CapEx model is much more tolerable for a lot of organizations.

I would suggest that everyone who is contemplating this move get help from an expert because the regular Azure and AWS cost calculators can be insufficient. Talk to Bill, talk to Josh, talk to whoever your adult is, to make sure what you’re doing is indeed the right thing. But in let’s call it 80% of use cases, it’s going to be a quick decision to make.

Bill: A lot of folks who have brought workloads back into hybrid or on-prem had a bit of sticker shock early on when they moved to public cloud. I don’t think it’s so much a reflection of public cloud, per se; I think they just didn’t build it out or architect it correctly, or at least estimate their cost correctly.

I’ve seen some horror stories on Wall Street of sticker shock, some very large monthly bills because you’re not paying attention to servers running 24/7, as opposed to just needing them two days a month. You need to be aware of your costs and know how to architect and tune it properly so you’re not spending an unneeded fortune every month.

Aftab: What are some functions that you might want to keep private?

Bill: Accounting teams like to keep accounting data close. I’ve seen accounting or batch processes that are running constantly, that folks like to have inside the walls, sometimes appropriately, and sometimes not.

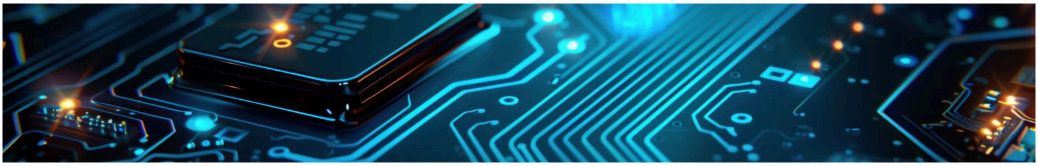
I think CRM has gone the way of email, where it’s commoditized and there’s a trust level. So, people are okay with their entire client list being in a CRM at Salesforce or whatever. It’s really a business discussion to say, “Hey, I think we could do it better, faster, cheaper, and more securely here, and here’s why.”

Gary: I would have named the same two. I have seen organizations have a top-secret security classification for some of their data. In a lot of those cases, they say, “I can’t have this in a multi-tenant environment.” More and more people are getting out of that mindset, but for a lot of organizations, that’s still point number one.

Aftab: Josh, you’ve heard the comments. What is your view?

Josh: Where you put your accounting data is a business discussion, to Bill’s point. As more and more people get comfortable with it, they get away from the idea of the cloud as this big, scary thing that hangs above us, and they realize it’s just a data center with ‘Microsoft’ stamped on the outside of it, instead of Equinix or anyone else.

So, you need a discussion with the business about why moving to the cloud will eventually be what all of us do, be it the accounting team or the top secret files that are encrypted somewhere else. I think everything will eventually get there. We just need to educate the people who think their data isn’t protected as well as it should be or it’s going to go into this mystery bucket of the cloud.



Aftab: What reservations do you encounter when discussing a greater reliance on public cloud?

Bill: Cost comes up within discussions. Are we going to spend a lot more to do this in the public cloud? And data security. However, to Josh's point, people are much more comfortable with moving to the cloud because of the maturity it's achieved over the past several years. Also, you'll see Microsoft and Amazon setting up parts of their data centers with NSA-level security. Not that companies necessarily need that level of security, but they now have that option.

One discussion I have all the time is that we'll have data for a particular client in a cloud at Azure. I back up to a second cloud on Amazon with different encryption keys. I can do it really cheaply in Glacier. So, let's say Microsoft goes down – it's not going to, but just suppose. Well, we've got a tertiary backup on AWS, and it's encrypted with different keys. So, this multi-cloud strategy gives people peace of mind when it comes to discussions about security.

> "Voice cloning is a big problem.... AI has made that possible.... You really want to engage with your employees and make them aware of their importance. They're the first line of defense."
> **Bill McSorley**

Gary: Yeah, I've done the same thing. In fact, Josh's team has done a lot of that for us, where we've got primary in the public cloud, we've got secondary elsewhere, and tertiary copies that we can rehydrate and bring back online if need be.

But that's no different than how it was with an on-premise situation where you had to have your DR site; you had to have additional copies somewhere. It's just there's a lower probability of these larger offerings going down.

I think we've all experienced the smaller data closet that has the outage because a rat chewed on a wire, or an AC broke. With data centers of this scale, you don't have those issues anymore.

Aftab: Josh, you facilitate so many cloud migrations and do so much work with public cloud. What improvements are needed to make it more suitable for private equity firms?

Josh: I don't think it's a technology thing. I think it's a trust thing now. Ten years ago, everyone was very anti-cloud because you're giving your data away. Now, we need to get past that concern with people who are not technology first. It's about convincing the accounting team or someone who's got a secret file that it's still in a data center, it's still on disk somewhere. It doesn't ethereally exist. So, we need to get the trust of the non-technical folk that public cloud is the future platform. Between Microsoft, Amazon, Google, and the other niche players, no one's going to be able to compete with it.

Aftab: So, trust is critical. What else would you highlight?

Gary: I'd say training as well. A lot of teams are not there yet. But the manageability aspect of public cloud is delightful. It's just that rapid development sometimes falls out of sync with our standard methodologies, where I could go into PowerShell or Exchange 2010 and remember all the commands. Now I go into Exchange Online, and suddenly that button isn't there anymore.

Bill: Yeah, it's a challenge when a command that worked in the last version of PowerShell doesn't work. That's a little frustrating, but it's par for the course. But yes, I agree with Gary and Josh that it's a trust thing. It's educating people that their data is encrypted and saying, "Look, if worst case, someone breaks in, they still can't read your data."

Aftab: What strategies do you use for cyber testing and ensuring everything is up to speed at the portfolio company level before and after acquisition?

Gary: We take a multi-phased approach. Cybersecurity is 1,000 items long, so it's a question of what are the most important things? What are the easiest things to implement? Things like vulnerability assessments, cybersecurity awareness training, and making sure there's phishing testing going on. I've got like five things up front and 14 things as phase two, everything from ensuring there are periodic penetration tests going on to making sure they have BCP plans and incident response plans.

Ultimately, it's about picking out a small subset of things for people to focus on. And even if you don't get it perfect, doing it to the 80th percentile, the 90th percentile is far better than not doing it at all. So, at some point, it's getting over the analysis paralysis and just doing it because whittling away at the risks on that list is really the best thing you can do.

> "I will say that some of the happiest days of my life were the days that my sons were born and the day that we got off Exchange on-prem."
> **Gary Marshall**

Aftab: Bill, what are some of the items on your list?

Bill: The one thing I do right from the outset is get the support of the founders or the senior partners at the PE firm. When I meet with them, I have two columns: "Here's what you need to do, and here's what's going to happen if you don't do it." And you show them horror stories from the front page of the *Wall Street Journal* of when you get breached, and you're being sued, or you're being fined by the SEC. And so, you adopt a proven framework, a NIST or CIS.

I'll give you another example. My technical DDQ that I send out to portfolio companies is 80 pages long. They hate it when they get it. And so, I've learned over the years that I don't send all of it to all portfolio companies. I've got different versions that are most appropriate for what we're looking at because if you address the low-hanging fruit first, you're going to be much better off.

Aftab: All right, fantastic. Josh, you said public cloud is the answer to many of these challenges. Is it also the answer to cyber?

Josh: It's probably part of the problem with cyber, as well as being the answer. People can run things in public cloud very, very quickly, for brief periods of time, and pay very little for it. They can use public cloud to attack people quickly and disappear. People will weaponize it, and it's very difficult to trace that down.

Also, using public cloud and AI, we've gone from having emails that are spelled terribly with horrible domains and ridiculous naming conventions sent to our users, to ones that are now in better English than I speak, written very, very well with domains that are designed to phish users. So, there's always an opportunity somewhere, on both sides of the coin. With public cloud, we can use it for good and bad, and it's very powerful for both.

Aftab: That sounds terrifying. What should firms be doing?

Josh: You need to make sure your user base is trained. If they get an email from out of the blue saying, "Oh, we need to close this deal immediately, text me this to this cell phone number; I've lost my other cell phone." There need to be enough red flags going in their head so that they don't blindly follow it. Your CEO is not texting you from his wife's phone telling you to just wire money!

Someone could send you an email from a domain that's very close to the right email address and can speak like someone because they've got some of their emails and learned their vernacular. So, make sure you ask questions and train your users to protect themselves.

Bill: Voice cloning is a big problem. I voice-cloned the CEO of a company that's a client of mine and used it as an example in cyber training for the employees, and he was stunned. AI has made that possible – it wasn't possible five years ago. It is now much more sophisticated, phishing, spear phishing.

You really want to engage with your employees and make them aware of their importance. They're the first line of defense. And make training interesting and engaging. Don't just go through dry facts and figures. You can't understate the importance of user education.

Aftab: Gary, what sophisticated threats have you encountered recently?

Gary: There's been some very, very interesting ones and some remarkably unsophisticated ones, like the free pizza phishing attack that was said to be the most effective at getting people to click. It had an obscene degree of success.

I've seen instances in the news about deep fakes. An employee at a firm got a voicemail from the CEO's phone number, from someone claiming to be the CEO, asking for something like a quarter of a million dollars. The employee put it through right away and then a couple of minutes later, thought, "Well, wait a minute, hold on, this doesn't seem quite right." He called the CEO and confirmed, no, that it wasn't him. But there's $250,000 you're never going to see again!

There was another one earlier this year where a large sum was lost in a similar scheme, using deep fake technology to pose as the company's CFO on a video conference call. The stuff you can do is obscene – the fact you can't trust the metrics we previously would have used to verify the veracity of a human being. It's pretty nuts.

When these stories come up, I send them to my user base, like, "Check this out. You're not going to believe this, but someone was able to pull this off." And that just helps build up their awareness, so they're that much less likely to be nailed by one of these things if one ever hits their inbox.

So, it's about training, training, training. We implemented cybersecurity training maybe eight years ago, and I've had to bump up the degree of difficulty because no one would fall for my phishing tests anymore. It's been very gratifying and very beneficial because the sophistication of these threats has greatly accelerated.

This is an edited transcript of a Private Equity Wire webinar Linedata sponsored in September 2024. Watch the webinar.

Josh Barber co-heads Linedata's Technology Services business, which includes Public Cloud, Cybersecurity, and Managed Services solutions for buy-side firms. He's spent two decades building and managing IT service organizations and delivery teams in North America, Europe, and Asia. Josh is passionate about delivering world-class IT services and solutions that address the unique requirements of asset managers, hedge funds, private market firms, and other financial institutions.

Gary Marshall is the Director of Technology at Paine Schwartz Partners. Mr. Marshall joined Paine Schwartz Partners as a Technology Consultant in 2013, and in 2015 he joined full time. Previously, he worked for an MSP in a variety of hedge funds and private equity firms in New York. He began his career at Bridgewater Associates in Westport, Connecticut. Mr. Marshall holds a number of industry certifications and a Bachelor of Arts in Economics from the University of Alaska.

Bill McSorley boasts an impressive background in the technology industry, spanning over two decades with a primary focus on financial services. He has gained recognition as a distinguished speaker at numerous technology conferences, a published author, and a respected member of the Forbes Technology Council. Currently, Mr. McSorley holds the esteemed position of heading WM3 Group LLC, a leading advisory firm that specializes in providing strategic counsel in areas such as cybersecurity, AI, compliance, and Fractional CxO services.

Learn More

Explore Linedata's private cloud, cybersecurity, and outsourcing services at www.linedata.com/globalservices.