Davis Hake:
The attackers inherently have the upper hand as they're looking to damage and break the systems. It's not just how you protect from attacks but how you build resilience against them. This might be, this might be strange for a cybersecurity expert to take this position.

Davis Hake:
Certainly, I do remember a day when I had to go to the library to check out physical encyclopedias or my books. Still, having grown up with the internet the majority of my life I have been accustomed to, and I think younger and younger folks are accustomed to, the internet being an open place and that the structure of the internet being distributed and being open for use is the fundamental benefit of this system. And it's what is driving the fourth industrial revolution that we're going through right now. You could say designers, should they have made it more secure from the outset? Would that have been a trade off in all the benefits we're seeing today? Hard to tell.

Jason Lopez:
Davis Hake is a lecturer at UC Berkeley School of Information where he's taught courses in managing cyber risk. And he's the co-founder of the firm Resilience Insurance. This is the Tech Barometer podcast. I'm Jason Lopez. This is one of those "how to re-think about something" stories. In this case, we're picking Davis Hake's brain about his thoughts on the fundamentals of security in a hybrid multi-cloud world. We'll get to that in a moment, but let's complete his broad brush view about the openness of the web and the trade off of the benefits versus the vulnerabilities. He says we've put a lot of emphasis on the benefits but maybe haven't given the realities of the vulnerabilities as much thought. Hake thinks that security on the open seas of the web should simply be a part of operations.

Davis Hake:
Okay, we've built this system and this network. How do we stop users on this network from harming each other over this network? And I think that we need to not just think about vulnerabilities and patching vulnerabilities but how do we start building products and ecosystems that help protect the users that are using them in a way that the system can still be open and accessible, and still encourage innovation and, and drive sort of our global economy

Jason Lopez:
So let's drill down into the enterprise. Here's the example, the mitre attack framework, which basically approaches security from the point of view of the intruder instead of an engineering approach, attempting to fortify everything, it asks the question, how would an attacker compromise and use the system? The answer to that question generally starts by prioritizing security measures aimed at protecting vulnerabilities likely to be most damaging to the business or to customers. The to do list might start by limiting the attack surface or putting protections in place to limit attackers from moving laterally or escalating privileges. Hake emphasizes that as much as we've put into the prevention side of security we need to think about realities. As much energy needs to be put into the recovery side.

Davis Hake:
This is where we're seeing a lot of research done by our data team and all the industry at large in saying what are the best investments? So that if there is an incident it's contained, your security technology has limited the damage that it would do to a network. And that if there is a bit of catastrophic damage, what are the best practices for coming back, for taking that punch and standing back up in a way that it actually is probably stronger than you were in the first place? Because post incident you know lot about these vulnerabilities you might have had. And you're looking at putting a lot of more investment in the places that maybe previously you had overlooked.

Jason Lopez:
Hake says cloud native has revolutionized enterprise computing, especially for startups where it's economically and security wise, significantly easier, especially not having to deal with legacy architecture. It allows a company to launch a new production environment with less effort than compared to trying to keep older equipment and systems working.

Davis Hake:
Hey, there's that server from ten years ago that we completely forgot about but is still attached to our entire backend email system and is a vulnerable point of our attack surface. So I think being cloud native has been a game changer for startups but also for small companies too that don't necessarily have to invest in the hardware and then keep that hardware for years to recoup that investment. They can deploy a new system. They can shut it down if they don't need it anymore and jump in to something else.

Jason Lopez:
So now the questions of the hybrid multi-cloud. We're in a moment of development in which most companies, even governments, are not betting on one cloud provider, but using different systems, working together, whether owned or rented. And now during the past couple of years of a pandemic, this energy has been accelerated as many companies ask, how do we move everything to the cloud?

Davis Hake:
As a startup we've been cloud so we've developed a lot of our security policies around that from the start. But you're an environment that's, you knows, um, you know, uh, there's a lot that you have rethink your security strategy, right? And so I think that that is where a lot of the security conversations that we talk about with our students, Berkeley come in in saying, you know, security, isn't something you can set forget, right? Technology is going to change. And it's your responsibility as the, you know, that essentially owning cyber risk to enable that technology to be used in a, in a safe way, right. It's not to turn that technology off, stop it from being deployed, but it's, how do you consider the risks and adopt your investments to, to mitigate those risks? And I think, you know, when you look at cloud that way, right, there's actually a lot that can be leveraged to help secure systems even better, um, through the cloud, right? I mean, this idea of, um, shared responsibility where, you know, cloud providers are responsible for the security of the cloud, your entity is responsible for the data in the cloud and

use of the cloud, right? Um, that's a strong core concept that it, if it's not understood, <laugh> can lead to, you know, problems at scale, but if it is well understood, it can lead to incredible results at scale, and it can make a lot of old existing it practices, uh, exponentially easier to secure systems, right?

Jason Lopez:
The anxiety of putting your data in the public cloud is the, and of whether it's secure to which ha says it's very secure because many companies are on multiple providers for different things.

Davis Hake:
It's not just like everybody is on one provider. Everybody is on multiple providers for multiple different things. Right. And, and that actually, I think provides sort of a security ecosystem such that, that, you know, you are, are more resilient by having more of these options. Um, but on the other hand, too, like that, that does mean that you have to invest in thinking through how do you deploy, um, certain, a assets that, you know, should only be accessible internal to your company, or that need to be served external only. I mean, you know, one of the, the common breaches that continue to see are, you know, misconfigured as three buckets, right? And, um, <laugh> leaving, you know, systems exposed with default credentials and password even still that, you know, people believe our development environments, but, you know, they're accessible in a way that, you know, something might be for, um, for sharing or something that production and meant to be client facing, but, but shouldn't be right. And so I think that this is an area too, where there's been some exciting work in a startup space around here. Um, but it is something that, you know, cause it's not traditional physical systems, um, you know, CISOs really have to be experts in cloud to a, to have to have a secure company.

Jason Lopez:
And speaking of expertise, one of the critical issues that hake says every business should practice is that cyber risk ought to be a conversation at the board level. And what he means by that is security should not be something just left to the it, people hired to do security decision makers, much less us, everyone in the company might have no expertise in the technical aspects of security, but they ought to be involved in it.

Davis Hake:
There are a lot of things, uh, that have driven risk management at the executive level, serving Oxy, for example, and more and more right. Every company has a, a digital footprint, every company, uh, you know, even, even Bob's pizza around the corner, uh, relies on the internet to enable their business. And, and so digital risk and investments in having your, your company operate safely should be seen as a, as a core priority, not just as a cost center, um, you know, from the it department that wants to buy, uh, a shiny new security toy, right? Like we really have to think about, um, about how we not just, uh, you know, physically ensure supply chains, uh, management of products. We also to need to think about how we secure ourselves and our customers because we're seeing more and more cases where those investments aren't made and the consequences aren't just catastrophic for a company, but have national impact.

Jason Lopez:
Davis Hake is a lecturer at UC Berkeley's School of Information where he's taught courses in managing cyber risk. And he's one of the co-founders of Resilience Insurance, which insures and secures companies from cyber attacks. This is the Tech Barometer Podcast produced by The Forecast. I'm Jason Lopez, thanks for listening. We've got more stories about tech and the people in technology written by great writers like Tom Mangan, Joanie Wexler, Gene Knauer to name a few. You can check them out at theforecastbynutanix.com.