Deloitte.

The Deloitte On Cloud Podcast

David Linthicum, Managing Director, Chief Cloud Strategy Officer, Deloitte Consulting LLP

Title: **Cybersecurity: Customizing risk management for your enterprise**

Description: Cybersecurity is top of mind for most organizations today, but it's a multi-faceted, challenging issue. In this episode, David Linthicum and Deloitte's Justin Rowe talk about the importance of customizing cyber and data security to fit the vision, risk environment, and culture of the enterprise. They also discuss trends in cybersecurity—including the rapid emergence and benefits of artificial intelligence as a way to increase the effectiveness of cyber risk management.

Duration: **00:24:07**

David Linthicum:
Welcome back to the On Cloud podcast. Today on the show I'm joined by Justin Rowe, managing director of cloud security and data risk. Justin, welcome to the show.

Justin Rowe:
Awesome. Thank you for having me today. Pleasure talking to you again, David.

David Linthicum:
Yeah, one of the things I was looking forward to today is to get a perspective in what's going on, get an update in how security is, what we're thinking about in terms of security. Seems to be just an ongoing process in the fact that we're always going to have to do battle with security systems. Certainly, the cloud is going to be no exception, and the evolving technology, really, around the emerging and changing threats is something that's going to be ongoing. Am I overstating that risk?

Justin Rowe:
Definitely not overstating it. Actually, it's a message we're always trying to propel to our clients, so you're spot on.

David Linthicum:
Yeah, and I think we're going to see some security issues start coming up around the use of Generative AI and the ability to weaponize this technology against many of the enterprises out there and of course leveraging AI-based systems or AI-based security and looking at that as well and the ability to use that as a defensive mechanism. So, it's really going to be an exciting, evolving space, so you're pretty much where the action's going to be. So, tell us how you got to Deloitte. What's the Justin story? What happened before you got here?

Justin Rowe:
Yeah, certainly. So, I entered the military in 2005. I joined the Air Force right out of graduating college in which my goal growing up was always to serve. When I entered the military, I actually was in the field of logistics with the Air Force, so not cybersecurity at the time. I spent about six years around the world, including the Middle East, in which when I transitioned out of active duty, I joined the reserves for a number of years, up until about 2016 but didn't get into the cybersecurity space until about, I would say, 2013 timeframe when a former colleague of mine, who was also in the military, was working for a managed-services firm here in Denver where I currently reside and offered me, “Hey, we're looking for leadership, we're looking for some team leads to help us around data loss prevention technologies, working with some clients across multiple industries, and would you be interested in just taking on a new challenge?” And, of course, coming from the military and that experience, who am I to say no. So, for the most part, I wouldn't say I found cybersecurity; it actually found me, and that happens for a lot of people that I meet.

But after sticking with the data loss-prevention capability from an operations perspective, helping our clients get their programs off the ground, that led me to an opportunity here at Deloitte where we were able to take the opportunities, and those that were experienced, within it to extend it to the cloud through the technology called CASB, or cloud access security broker, and helping build program off that since that's the technology that was taking off around the 2017 timeframe, 2016 timeframe.

So, I joined Deloitte then, and that's when I started venturing more into cloud security, generally speaking, not just within that space, but also around what the cloud service providers were doing around data protection, but also, around cloud security and working in the life sciences and health care sector, which is where my previous clients were residing when I was in that managed services firm. So, a little bit of a journey, and a lot of lessons learned and experiences along the way, a lot of colleagues that I met and helped me get to where I am, so it wasn't just myself, but also my family, as well as those professionals that I’ve come to grow and learn from, as well as continue to learn from within the firm.

David Linthicum:
I love the way you stated cloud security kind of found you. What was your interest in moving in this space? There obviously has to be some curiosity and some driving force to move you in a particular technology space. What was cloud security's appeal?

Justin Rowe:
Really, the appeal for me was, in the most part, when I was in the military as well as after school, I got into a little bit of self-learning around innovation, and not just responding, but being more proactive than reactive around where businesses are going from a digital and technological and transformational standpoint. So, based on serving more in the life sciences and health care space, knowing that the life sciences sector was a little bit more advanced in cloud than health care, I wanted to get a little bit ahead of the game on what's to come, because at some point, cloud was going to be a significant undertaking for the health care sector in which the pandemic of COVID-19 really drove the increased use of the cloud.

So, having advanced knowledge and experience within the cloud space from a security standpoint really kind of helped us position ourselves to work with our clients and help them be successful, based on really not just the decisions that they were making, but most importantly, how they were responding and reacting in advance to support the business in situations like this to be able to support business objectives overall. So, that was really it, and then everything just started to take shape based on adoption, other transformation initiatives such as migration, cloud optimization areas, as well as just really maintaining adherence and compliance across multiple frameworks. So, it was a multitude of things, but it all culminated to where we're at now.

David Linthicum:
So, let's talk about cloud security in general, and obviously different industries deploy it and leverage it differently. Can you kind of walk us through how industries differ in how they deploy cloud security systems and what their differences are and also what are the common patterns?

Justin Rowe:
Certainly. So, across industries, and I'll even speak at a high level on just the adoption of cloud, is when organizations, whether they're using software-as-a-service all the way down to infrastructure-as-a-service, there's what is called a shared-responsibility model that organizations must adhere to, and that's by contractual nature of, “What am I going to be responsible for securing a virtualized environment across a number of cyber domain areas to include identity and access management, data protection applications, security operations, as well as resiliency versus what is the cloud service provider's responsibility

going to be?" And based on the direction that industries are taking, some are much faster to adopt based on the business, of course, and wanting to attract new customer bases, build new products, and get them to market.

But most importantly, the visibility and management of risk, so that's what we're in the business on the Deloitte side is helping our clients understand managing cloud cyber risk from the get-go and driving, really, a culture of getting cloud security to the table up front based on business requirements, business development and ideation, as well as what is it that from a security standpoint we need to do to measure risk and identify the appropriate controls to do so. So, industries across the board vary in maturity. I even speak to clients today that are still trying to figure out their cloud strategy, whether or not they even want to move to the cloud versus clients that have been in the cloud for multiple years, have been doing this for some time, have very high mature areas such as automation, even machine learning in place. So, it varies across the entire spectrum.

David Linthicum:
Yeah, one of the things that we do is we don't push cloud, we push solutions. Your ability to kind of look at where your assets need to reside, and that's going to bring the most value back to the business. And it seems weird, everybody seems to be moving toward the direction of cloud, and lots of good reasons for making that happen, but you do have to kind of take a stepwise approach to make sure you're not making some mistakes. And as we're seeing now, people are hitting the reset button and repatriating some things right now because they moved workloads that shouldn't be in the cloud. So, do you think that the money being spent across the industries is consistent? I would say probably not. And where are people typically underspending and overspending on security?

Justin Rowe:
So, a lot of chief information security officers will probably always attest to needing more budget. There's always that opportunity to do more with more, but at the same time, the challenges have been recognized, at least from my standpoint, over the last few years, of it's not just a technological problem. Cyber risk needs to be managed through people, process, and technology in which, traditionally, we've seen areas of governance, for example, where clients have attempted to basically replicate what they've done on premises for a number of years into the cloud, and that just has not been successful. It's not like a one-size-fits-all, so if, David, you come to me and say, "Hey Justin, I like your suit." Well, I can't let you wear it because it doesn't fit you. It won't fit every single organization one-for-one, so it really depends on the tailor who built it.

So, based on industry frameworks and standardized capabilities, that's one step to get there, but from a people standpoint and how we govern and have visibility into the cloud, that's where things start to change. We start getting into processes of adoption such as DevOps, into DevSecOps, automating through pipelines and building immutable infrastructure and deploying customized and unique templates based on those business requirements to where we can try and standardize through code as much as we can, but also at the same time continuously have observability and monitoring for new cyber risks based on changes within the cyber risk and threat landscape. But, also, where one of the highest areas of events or incidents that take place is misconfiguration.

So, there's a multitude of things where clients are spending their dollar today, and a lot of it tends to start natively through available security controls and then extend into whether they're using different types of products, whether they're converging into a single capability such as secure access service edge or secure service edge which hones on looking for misconfiguration, enabling secure web gateway, data loss prevention, as well as driving, logging, and monitoring across the entire cloud landscape and their infrastructure and platform as-a-service capability. So, different clients are spending their money in different ways.

And then the last part I'll say about that is, going back to your example of where they're at in their journey. We want to meet our clients and help them get to where they want to go, especially around where the business is going. Working with clients that have a perspective of lift-and-shift and they want to move their workloads from their data centers—offload their data centers and just leverage infrastructure and operating systems virtually, versus clients that have a no lift-and-shift strategy and they just want to leverage cloud services for development and hosting data only. So, again, depending on the client, depending on the direction they want to go, is where we've seen security need to be managed in different ways.

David Linthicum:
So, I'm a new client, walk me through the process of understanding what the use cases are, how we should leverage the technology correctly, and how to work to an appropriate cloud security framework that's going to have the best chance of success.

Justin Rowe:
So, from a security risk standpoint, and within our advisory practice, we're always pushing to embed ourselves into cloud platform teams and enterprise architecture organizations where they receive requirements from the business on the use and future consumption of cloud services, and from that area, at least from the development of a cloud vision to defining what a cloud pilot or proof of concept is going to look like, the initial use cases of what it is that we're going to secure has to be brought in from the start. Security technically and traditionally and always should not be an afterthought. We always want to bring security risk up front because, again, we're in the business of risk management, and not just from a cyber standpoint, but also from a financial reputational risk perspective, as well.

And then, of course, messaging that to our clients to say, "Hey, we are using these new digital capabilities and we want to drive trust toward our customers." So, different use cases, of course, will allow for an assessment of risk to be adopted. So, one thing that we're seeing quite a bit of, and the increased execution of it, is the process of input through a service catalog of requesting the adoption of a new cloud service to be sanctioned within the organization, in which a cybersecurity team does an assessment again. And what we mean by that is what are the appropriate controls to maintain confidentiality, integrity, and availability of networks, infrastructures, and even data? And what controls do we have to put in place to minimize impact, as well as reduce probability against the direction that the business wants to go from an overall cyber risk standpoint?

So, based on that step in the process of adopting cloud, we're seeing a significant increase in that learning, based on not just it being a standard governance capability, but more or less a part of the culture in which, previously, going back to my cloud access security broker example, the initial use case was

monitoring for sanctioned and unsanctioned cloud. What SaaS services, what is the business using that may not have been authorized where data may have been exfiltrating and taking some sort of action to assess if that's authorized, and then, of course, having a list of sanctioned cloud services.

So, that transitions more into notification and behavioral changes within the organization of approaching security up front. I'll use the example quickly this morning when I was driving in: You're on the highway and you start to see signs of a lane being closed a mile out, a half-mile out, a thousand feet out, and then traffic just always weaves into one another and traffic still flows, versus, this morning, there was a sign that said the lane was closed immediately. There was no pre-warning and there was just a complete bottleneck. That's the bottleneck that we want to avoid in cybersecurity is giving an on-ramp to the organization on how they adopt cloud services from a secure standpoint up front.

David Linthicum:
Yeah, I love the fact that you mentioned vision. I think that sometimes is missing—what we need to understand about cybersecurity, people like to throw tools and technology at it, and I understand why they're doing that because that's where we kind of focus our efforts and our innovation, but the ability to have a vision as to where the business is going is something that I think is missing from many of the conversations when we talk about anything, including architecture and security solutions around it. Also, I like the fact that we're now engineering security into the applications, into the workloads, and into the culture, which is something that I also think is hugely missing, and is going to raise a lot of risk in value in the marketplace. And I think enterprises are slowly moving in that direction, more or less trial and error, and, so, it's something that really, really should be focused on. What are we doing right now in terms of data security in the cloud?

Justin Rowe:
So, the important part of the conversation up front around data, we tell clients it's always about the data. That's what they tell us and that's what we tell them. The most important part about data is—and this goes across what we call the data governance umbrella, which contains data management, data protection, and data privacy, is visibility. We can't govern, we can't have accountability of data if we don't have visibility into what data is where, who has access to it to include users, administrators, and even service accounts. We want that visibility; we need that visibility up front in order for us to discern what controls we need to apply to it based on the data risk that's being assessed against it.

So, based on data classification schemas that clients already have in place that could be extended to where data is hosted and processed and persisted in the cloud, as well as data dictionaries, data catalogs to include other controls such as encryption and key management. But based on our customers' requirements and how they have it documented within their policies and standards, such as AES 256-bit encryption based on industry standards, well how will that be applied toward the use of it within the cloud? And the cloud service providers are really good at providing those encryption requirements up front, but depending on your industry and regulatory requirements, then you start to shift on how you're managing those keys to encrypt that data to begin with. So, again, there's a little bit of a shift on how you do things in the cloud from a data security standpoint.

And the last couple areas I'll focus on here is, based on data in motion, or data in transit as some folks call it, how are we protecting against data exfiltrating from the organization. So, we always want to drive a process to our clients of continuous input and adoption of new data sets being created beyond just what is, from a compliance perspective such as protected health information, and leveraging the HIPAA compliance from a security, privacy, and breach notification framework standpoint, to intellectual property and what, basically, is the lifeblood of an organization related to making business decisions through analytics and insights, as well as always looking to create a competitive advantage and drive new value propositions to their customers.

So, any and all data, no matter what type it is—structured or unstructured—should have some sort of data protection mechanism around it to prevent the wrong data leaving the organization, whether it's malicious or whether it was by accident. So, in a lot of instances, we'll help our clients just transform their existing processes, and, again, that culture and behavior to focus on what those data loss prevention capabilities will look like.

And then the last part I'll say around data is retention and deletion. The more data you have the larger your attack surface is going to be and the increased risk that you have to manage against it. So, based on industry regulatory compliance requirements, you may have a specific number of years you have to retain that data. But after that time period is met, then what do you do after that? Do you delete it? Do you remove it? Do you move it to cold storage? There's multiple areas where you can leverage the cloud to do so, in which we want to make sure our clients aren't just holding onto data to do so without making sure they understand the risk implications behind it.

David Linthicum:
There's a lot to think about. So, let's talk about the trends in cloud security. So, where are things going right now? What are the vendors doing? What are some of the common emerging solutions that we're seeing and also what's the influence of AI in the world of security?

Justin Rowe:
So, when we talk to our clients about controls, and we'll focus on logical controls or technological controls to begin with, depending on the client's budget and size of their team, of course, to manage cloud security risk, is normally the first order is go cloud native. The cloud service providers have been consistently improving upon and building new security products built within infrastructure and even extending toward platform as-a-service capabilities to where it's very turnkey. And even if you're using it within the UI, you're able to design and drive forth security controls natively within a specific hyperscaler. Now, a lot of those security teams have been leveraging other third-party vendors for a number of years, have solid relationships—especially those that are very prestigious when it comes to their maturity as well as the ability to innovate and stay ahead of the pack—want to continue to stay with those vendors.

So, the latest trends around some of these vendors is this notion of convergence of capabilities where clients previously were just purchasing licenses for point solutions—whether it be a CASB separately from a DLP solution separately from an encryption capability or firewall intrusion detection, intrusion prevention-all the way down to security operations around vulnerability management and SIMS, or security information event management. So, multiple solutions scattered in your technical debt is just adding up. Now, a lot of these vendors are converging into a single platform, sort of like an end-all-be-all, and you always hear the single pane of glass type metaphor, but we're starting to see that a lot, and it's a little bit slow adoption, but a lot of these clients

are starting to adopt these converged products into a single policy to roll them out ways in which they don't have to rinse, replicate, and see multiple streams in order for them to take action.

You mentioned a little while ago about the inclusion of AI and the power that artificial intelligence has, and a lot of vendors are actually building into their products today a number of AI capabilities to help drive forth not just SAC teams to be proactive and reactive but really be predictive. And through different threat-hunting and threat-intelligence gathering capabilities, leveraging AI to discern, "Well here's an increased probability of this event happening," because we're starting to see new threat actors build new sets of malware or ransomware across the industry, and we're starting to share information across teams globally, in which AI is starting to detect and actually drive forth proactive action which controls need to be built, applied, tested, and operationalized. So, that said, we're also working with clients to help them understand what are the cyber risks of using AI, such as Gen AI, within their organizations. So, going back to the data security and CASB example, we want to have visibility into what the business is using from a Gen AI perspective to begin with.

That's where we can standardize and create that baseline on which policies can be built around. So, if there's an authorized process of Gen AI being used, we may want to prevent data protection controls in place to ensure that we don't have the wrong data going out the door and being sent to Gen AI capabilities where it's now in their environment, they have access to it, they're using it, and of course it's no longer just solely hosted in our network. So, there are abilities for us to drive forth controls through enabling the business but also making sure that we're protecting the business from itself at the same time. So, through those data protection controls within a CASB-like solution, we can help clients put in whether it's just detective controls only and reporting events to preventative and corrective, based on what is authorized versus unauthorized.

David Linthicum:
Yeah, I love the fact you're looking at this the right way and that we're moving to a proactive stance. We're able to leverage technology, not only to defend ourselves in procedural ways, policies, rules, and reaction to rules and policies, that kind of stuff, but the ability to kind of look ahead in terms of what patterns are leading up to a likely breach and the ability to take proactive response before something happens. I think by then it's too late, and the ability to kind of put up this proactive front is really the way to go, and AI is going to facilitate us in getting there in a much easier way because the power and the predictability and also building of the knowledge base is kind of innate to what that technology is. So, where can we find more about you on the web?

Justin Rowe:
Well, I have a LinkedIn profile, of course. Also on our Deloitte website based on some recent publications that I've supported as well. So, like I said, I mostly support our life sciences and health care customers, but of course, cyber risk is everywhere and we always want to drive forth that message to our clients, so there's always a need for a client to come to us and say, "Hey Justin, I want to talk to you about this specific question or scenario or even use case," we always have the right team members we can pull in to have that conversation.

David Linthicum:
Yeah, check out Justin. He's a smart person in the organization. Really glad to have him here. And also just understands a bunch about where this technology is going and just focusing on the space, and also he has real life experiences of working with clients on a day-to-day basis. I think that's most important, and lots of different domains. You're not just working for one company, but you're working with multiple companies and, therefore, your experience just really kind of multiplies pretty quickly.

So, if you enjoyed this podcast, make sure to like us, rate us, and subscribe. You can also check out our past episodes, including those hosted by Mike Kavis. Find out more at deloitteccloudpodcast.com. If you'd like to contact me directly, you can email me at dlinthicum@deloitte.com. So, until next time, best of luck with your cloud journey. Everybody stay safe. Cheers.

Operator:
