Architecting the Cloud, part of the On Cloud Podcast

Mike Kavis, Managing Director, Deloitte Consulting LLP

Title: **Making cybersecurity more effective in the age of cloud and COVID-19**

Description: Cybersecurity has always been a critical task that must be handled effectively. However, cloud—and more recently—COVID 19—have exacerbated cybersecurity issues and changed the security landscape. In this episode of the podcast, Mike Kavis and guest, Ascent Solutions' Kayne McGladrey, discuss cybersecurity in the context of cloud, and vis-à-vis the changes wrought by the pandemic. Kayne's take is that the transition to cloud and the pandemic have exposed and magnified issues that have always been a problem, and that companies should not skimp on cybersecurity, in favor of spending on other "more pressing" projects. The key to success is to focus on data, automation, and risk assessment.

Duration: **00:29:06**

Operator
This podcast is produced by Deloitte. The views and opinions expressed by podcast speakers and guests are solely their own and do not reflect the opinions of Deloitte. This podcast provides general information only and is not intended to constitute advice or services of any kind. For additional information about Deloitte, go to Deloitte.com/about. Welcome to Architecting the Cloud, part of the On Cloud Podcast, where we get real about Cloud Technology what works, what doesn't and why. Now here is your host Mike Kavis.

Mike Kavis:
Hey, everyone, welcome back to the Architecting the Cloud podcast, where we get real about cloud technology. We discuss all the hot topics around cloud computing, but most importantly with the people in the field who do the work every day. I'm your host, Mike Kavis, Chief Cloud Architect over at Deloitte, and today I'm joined by Kayne McGladrey, Cybersecurity Strategist at Ascent Solutions. And when I was researching you, there's 50 other titles you could probably throw on there, so tell us all the stuff that you do, because I know you're involved with a lot.

Kayne McGladrey:
Thanks for having me on the show too, Mike. It's a real pleasure. So, I am – at Ascent Solutions, my formal title is Architect and GRC Practice Area Lead, which is honestly too much of a mouthful for most people in the media to work with. And a lot of what I do when I'm not providing advisory services around cybersecurity, strategy, governance, risk and compliance to our clients is around public advocacy, which usually takes the form of media interviews, but also

public speaking. I'm really passionate about trying to encourage people from outside of our industry to consider careers in cybersecurity, which again, having a short title does help to make things a little easier. I'm also a senior member of the Institute of Electrical and Electronics Engineers, which is a fantastic organization to work with.

Mike Kavis:
Well, thanks for that intro. First topic I want to talk about, I saw you mentioned in an article called, "COVID-19 Pandemic has Become a Catalyst for Cyberattacks." And I'm going to get into one of the quotes you said in there later, but let's just talk about that topic. How has this pandemic kind of accelerated cyberattacks?

Kayne McGladrey:
So, I think it's necessary to differentiate between the perception of what's going on and the reality of what's going on, and I say that because the perception is that everybody working from home and COVID-19 has caused this massive uptick of phishing attacks where threat actors are sending these malicious e-mails to people who are unsuspecting at their home. And the actual truth of it, it's not happening at a greater clip. If you actually look at the statistics behind it, it's not really an uptick. What we've learned here is that threat actors tend to follow the news and they tend to follow the events of the day, and so just before the election in the United States, the FBI came out and said, look, all of those e-mails you just got if you live in Florida, or if you live in I believe it was Alaska, that are purporting to be from an organization threatening you if you don't vote a certain way, all those are from an Iranian threat actor that just doesn't have very good OpSec.

And I think that we've seen that throughout the course of realistically modern computing history, where if there is a hurricane or if there is a flood or if there is a pandemic or if there is an election or if there's anything else significant or topical in the news, threat actors are just going to go, you know what, let's just pivot that and make that part of our phishing campaign because people will click on that. Having said that, COVID-19 really has exposed some larger IT and cloud issues that are not so easily solved, and they definitely are on increase.

In March, in the United States, when many of us – almost all of us in some cases – were required to work from home, and some of us are still working from home, I think the challenge was that the supporting infrastructure for organizations just wasn't plumbed for at-home workforces. Let me give you a good example. IT asset management systems, often those are seen as a function of accounting, and they're not exactly your premier cybersecurity thing, but if you can't actually tell how many devices you have, it's very hard to actually categorically say where are all of your data. And if it's very hard to say what devices you have, it's also very hard to patch them. And as we've learned, patching all the things, whether they're on cloud, or whether they're endpoints that are deployed in people's homes or other network environments, is really necessary.

And so I think the lack of a consolidated view of IT asset management and the associated patching fall down of those on-premises solutions have required companies to either say (A) “Hey, you know what, could you pop around the office just once a month, put on a mask, show up, connect to a LAN and we'll patch your device,” which I think most people find unpalatable. Or (B) what we've seen out of, again, the bureau, which put out a list of the 25 most exploitive things that have happened this year in 2020, almost all of them are vulnerabilities that were exposed in this year. There's a 2015, but the majority of them top 25 are all this year. And a lot of them are around either border gateway devices, so those are your pulse secure VPNs or your other VPN providers. I think Fortinet was featured in there. Or it's all endpoints. And the reason for that is because we don't have good tracking at an enterprise level. So, when I'm talking to clients about this, one of the most easy questions that I can ask is you know, is your patching solution based on the premise that people can connect to the cloud and get patches, or is it based on them having to be at a place? Because if they have to be at a place, it's dead technology, it's a zombie, it just doesn't know it yet.

Mike Kavis:
Yeah, that's interesting. And to the first part of that where kind of the myth that they're doing more phishing because you're at home, I mean, they're just sending to IP addresses, right. They don't know who you are or where you are. But I think to your other point, the messaging is very relevant and people want to click on it. The other point, I wanted to throw this out there, is a lot of companies had to quickly pivot to work-at-home because work would stop if they didn't. So, they probably skipped a lot of steps to do that. So, talk about that a little. What did we really expose there and how long is it going to take some companies to actually button all those loose ends up?

Kayne McGladrey:
I think it's a question of where every company is in their security journey and what their regulatory and risk burden and contractual burden is associated with that. Some organizations, which previously–like a lot of startups these days—ultimately their office is a router and a coffee machine and some chairs, but actually all the work is done in the cloud. And in those organizations, even though they might not have a traditional CISO on the executive board, they usually don't hit that until they hit the mezzanine level, ultimately they're doing okay. It's those traditional castle-and-moat organizations where there was the belief that you go to an office and that's where work happened that are struggling the most because they won't have implemented things like a consolidated view of their assets, which makes it very hard to have a consolidated view of your software, and if you don't have those things, it's very hard to actually know where your data lives.

Because if you can't say, oh, it's on somebody's handset or it's on their laptop, how do you actually apply controls to that when you start thinking about things like data labeling or the movement of data around an organization, whether it's transiting endpoints or whether it's transiting to the cloud or not. And threat actors know this, and they have been exploiting that vulnerability to great effect because if it's possible to get a shell on somebody's VPN because they forgot to patch the VPN, that's not only a great lateral movement for them inside of an organization, but it's also a great way to do traffic inspection and to get signaling information, which if you're a nation state, that's super-duper interesting stuff to figure out who's doing what to who inside of an organization.

And as a result, I think a lot of organizations have struggled to put out temporary solutions. I've heard of hardware VPNs being deployed in people's homes. That's certainly an interesting solution. I've heard of organizations trying to move to an XDR model where their endpoint solutions are partially based in the cloud, but again, there's not really a consolidated view of what's happening in a lot of organizations. I think that moving forward, strategically speaking, the organizations that aren't doing, like, the Center for Internet Security's Critical Six controls, IT asset management, software management, patching, that kind of thing, get that locked down first.

But then after that, if you don't have a data classification and a labeling policy that actually work and have appropriate tooling, so that the end user doesn't find it onerous to label the data that they're creating and just the machine does it for you, which I find is a lot better. If you don't have that, stand that up because there's a lot of regulatory risk there regardless of regulatory regime, if you're leaking stuff, it tends to be a bad day in court in civil action or criminal suit, depending. But also, after that, if you don't have a consolidated SIM solution for event monitoring for security events in your organization, or even if you do, most of those are just the horrible box in the corner that goes beep that nobody wants to talk about. So, I think organizations really need to look towards maturing of SOAR, which is orchestration and response based on things.

And then the most evolved organizations really do need to move to threat hunting as code where it's no longer acceptable to do a threat hunt based on Mitre's attack and say, look, we think we're going to get nailed by Fin7, so let's go and build ourselves a hunt and let's pretend Fin7's coming after us, right, and do that on a Monday and think, great, we're done for the month. You're not. You should have that automated, that should be code, that should be something that can run. Because if you're not getting the feedback from your controls, your technical controls that, that is working, it's really hard to detect when an incident has occurred. And then if you look at things like GDPR, which has got a 72-hour breach notification window or something like a contractual obligation I saw which had a 24-hour breach notification window, if you don't even know you got breached and it's going to take you months to figure out, you're going to have a bad day.

Mike Kavis:
Bad few days, yeah. So, the other issue we had is we pivoted real quick to work from home, but a lot of companies are in industries that are getting decimated whether it's travel, food, things that their revenue's going down a lot because there's not as much business, so they've got to cut budgets, so they've got to kind of balance some of these security projects versus other projects. And even the ones that were doing good, like some of the shipping companies, they're doing really good, but they're dealing with scale that they never had to do, so that's a priority. So, there's this prioritization, there's all this security threats going on, and we've got to juggle the limited dollars with security projects versus other projects, and you had a great quote in there saying, "Delaying or canceling security projects is an acceptable tradeoff only if bankruptcy is your alternative," which I thought was a great quote. So, speak about that.

Kayne McGladrey:
So, I think that if you – look at it this way. The number of regulatory and legal requirements that have been turned off where the regulatory body or some politician said somewhere, "Oh, you know what, let's not do that anymore, that doesn't make sense because COVID," right, or because, as my kids would say. There's zero. OCR has reduced enforcement of or relaxed enforcement of HIPAA temporarily, but that's' it. Realistically speaking, if you are in a regulated industry, like let's say you have to comply with New York Section 500, which their attorney general is currently doing enforcement of New York Section 500, or if you're subject to the CCPA, which in California the attorney general just in July spun up enforcement actions against organizations for violating CCPA, the privacy act. In both of those cases, it's not because COVID is happening, ergo we can just let stuff slide. And that's just from a regulatory perspective.

On the other side of that, the ransomware threat crews are doing very well for themselves financially during this time, and they are certainly looking to increase their revenue even though right now it's kind of a holding-shells organization setup financially. It's very hard to get the money out if you can't get money mules because people on the street look suspicious, which is currently an economics pattern and problem I think they're still working to solve. But the challenge is that if you are looking at either disabling security controls, or not implementing security controls, especially those around right now the current hotness of prevention of data exfiltration and doing good backups, then realistically ransomware becomes a substantial threat to an organization.

I was recently talking to a manufacturing company, and their challenge was that they'd had a negative interaction with a cyber adversary associated with ransomware, and the amount of money that the ransomware threat actor wanted to charge them would have put them out of business. And if they did not have good backups, they would have gone out of business. And then if you look at, okay, say maybe they didn't have good backups, maybe just as a what-if. If they didn't have good backups and they had to actually pay the ransom, if you look at what Treasury has done just recently with OFAC coming out and saying, look, we saw you, Garmin, we saw what you did there, we don't think this is funny by paying Evil Corp via third party, and Evil Corp is on the US sanctioned entities list, Evil Corp—great name for a Russian threat actor group. I love that one.

Anyway, they basically said, you know what, the next one of you who does this, who actually pays a sanctioned entity, even if you don't know that they're a sanctioned entity, we're going to come after you with a $20 million civil penalty. So, now when you're doing that weighting of scales associated with cybersecurity controls, you have on one hand the cost of whatever the vendor is charging you for that control framework, as well as implementation and ongoing maintenance and subscriptions and whatnot. And on the other hand, you've got to balance that against what is your insurer going to pay, and what are the potential civil penalties, whether they're brought as part of a class-action lawsuit or whether they're brought as part of a legal action by an attorney general, and what Treasury might do to you if they're feeling particularly persnickety on that day.

And the other thing I'd say as well, there has been this tendency to say, oh, well ransomware, it's covered by our cyber insurance. And to that I'd say the debacle of *Mondelez v. Zurich* is really informative. And for those listeners who aren't tracking *Mondelez v. Zurich*, Zurich Insurance, they're an insurer; Mondelez, they make snacks. They got ransomwared, but it was actually a data wiper, and it was attributed to a nation state. And because US Cybercom attributed it to a nation state, Zurich, their insurer, said, "Ah, you know what, that's just an act of war. Those aren't covered by insurance. Sorry." Which Mondelez, they looked at that and went, "Um, didn't we have insurance for ransomware and stuff?" And that is a really important conversation that I'd encourage everybody to have with their insurance brokers at this point is to figure out if Cybercom does attribution to a nation state, are you still covered? And that could be against business e-mail compromise, that could be against ransomware, that could be against any other type of malicious cyber action to find out if a national attribution is going to cause additional downstream risk for you.

Mike Kavis:
Yeah, as an app developer, there's a lot of stuff going on there– we're blind to, right, because we're focused on business requirements, delivering features, and there's all these people have got to deal with all these threats. It's amazing how much bad people – bad actors can do. It's really incredible. I was once at a data center, an office of one of the cloud providers, and it was in UK at the time, and they had this huge monitor that showed the whole world, and it showed their data centers, and it showed threats coming in, right. It was like little meteors. And while we're sitting there talking, all of a sudden the map just flooded. They were getting a DDOS attack. And it was just like millions of lines came from one part of the world to this data center, and they – at least from the map, it looks like they defended them all, but it was just amazing. We were just sitting there and it's like little meteor, little meteor, all of a sudden

whoosh, like the whole half of the world turned white stripes, right, as all this stuff was going on. And it was just another day in the life of a cloud provider having to deal with this.

Kayne McGladrey:
Absolutely. And I would say, you know, years ago, back when dinosaurs roamed the internet, I actually used to bang code for a living, and something that I'd like to emphasize is that there is a responsibility model on the course of application developers, but it's not what you'd think. What most people think is, okay, don't allow buffer overflows and check your inputs and, yeah, sure, those are all good recommendations. The thing that we're seeing primarily as a risk is around supply chain, in the code supply chain, because most application developers just don't have enough time. Actually, I think I can back that up. Most people don't have enough time ever really, and as such, a lot of commercial products are incorporating open source software. Now, open source software components, not bad. Totally fine.

Actually, I tend to use a lot of them myself. However, no single entity is doing code inspection against all of those open source components for vulnerabilities, and if you're shipping a service or if you're shipping a piece of software that has incorporated those vulnerabilities in it and you don't have a good software manifest, that means you're actually exposing your clients to additional downstream risk because you've shipped a manky piece of code that you didn't make, but does the thing you need it to do. You're seeing that this week with, like, the electron framework on Discord on desktop, which has got a remote code execution thing, which you go wait, how does that even happen. And it's not because the people at Discord were sloppy; it's because they incorporated just an open source framework.

I think that from a contractual standpoint, taking that back to the business level now, what we're seeing is requirements. These are primarily in the banking and computing section as well as the defense industrial base for application developers to provide a code manifest of all of the components that make up part of their code. And by doing that, they at least know, okay, do we have a vulnerability associated with that? The alternative, the flip side of that is to pull an Experian where they had an old Apache Struts machine that they only just kind of realized that they had and then they decided, ah, you know what, we don't need to patch that. It's fine. Which again, they had a fairly bad time and their CISO also had a particularly bad time up on the Hill.

Mike Kavis:
So, let me ask you a question about that. Getting specific about cloud, one of the things people who don't have time, we want to write less code. We want to get stuff to market faster and we want to leverage what's out there. So, a lot of times we leverage these managed services. So, if you think about a database, an Amazon RDS, right, so it's a fully-managed database. I don't do anything infrastructural with that. I'm just building code on top. In that model – I don't know if model's the right word, but in that scenario, does that actually make us safer because companies like Amazon, Google, and Microsoft are, that's their core competency and they're working and making sure that all those protections are down there. Does that actually make us safer than when we're rolling our own database technologies on our side?

Kayne McGladrey:
I'm going to say yes-ish, and the -ish there is important. It's not quite a firm yes. I think a lot of magical thinking exists around the shared security model where companies feel that by lifting and shifting, whether they're infrastructure is a service or they're backend databases to infrastructure that's hosted in the cloud, everything magically goes away, and it's really important to understand the shared responsibility model that yes, if you're using a platform, the hosting provider, the cloud provider, is going to take care of a lot of the stuff that's not a competitive advantage. They're going to take care of, let's say, patching of those servers. They're going to take care of actually making sure there's enough disk space available and the memory and all the stuff that honestly nobody wants to do anymore because it's not a competitive advantage. However, they're not going to take care of your data security model or your user identification and authentication or privilege access or doing any kind of inspection of traffic to see, hey, is this an appropriate person getting into this machine and getting into this data set or is this something that's not appropriate? That's usually where the shared responsibility model stops.

And then also, depending on the nature of the data that are being stored, there also can be additional regulatory or legal concerns. I was talking to a client that handles defense industrial base information, and their plan for migration to the cloud was that they had a whole bunch of on-premises e-mail servers. They're like, you know what, we don't like this anymore. We're just going to move it all to the cloud. And they didn't have any data labeling in their environment, and they – you know, they thought they might have CUI, controlled unclassified information, and they might have had some in their e-mail. But you know what, we'll just lift that and shift that up on a commercial cloud provider. It'll be fine. And then you go read DFARS and then you go look at ITAR and you find out, okay, that's probably an export.

You're probably going to have a very terrible time of it, and if they had instead said, You know what, let's take a second, let's troll through our data and see what have we got here, what regulatory controls apply to this, and this is as applicable for healthcare as it is for defense industrial base as it is for anybody handling personally identifiable information." Take a quick comb through it. Goodness knows there's enough automation in this space to do the work for you, generally speaking, with a high degree of efficacy. And then look at your cloud hosting – your cloud platform provider and say, look, do you have an appropriate option for that? Because in just thinking of this, like Microsoft for example, pick on them for a moment, they've got commercial Azure. They've also got Azure for Healthcare, and then they've finally got Azure for Government. And from their perspective, under Azure for Government, for serving the defense industrial base, the reason you can't use standard commercial Azure for hosting DIB data is associated with the right of the US government to show up and to roll through your servers and just kind of comb through.

Plus, there's also requirement for only US nationals to be working and have access to those. Those aren't technical controls by any means, right. The ability of the US government to do forensics theoretically on a hard drive in a data center somewhere, it's probably low probability, but because they're shielding themselves from litigation associated with that, they're saying, "Look, contractually you don't need to do this." So, as organizations are looking to move things to the cloud, yes, it can be more secure if you understand what the cloud provider is and isn't doing and also what they are and are not providing, and then you can make that decision, is this the right time to move this or is this something that we still should keep, whether on premises, or in an existing enclave environment where you already have those data controls and protections in place.

Mike Kavis:
So, last question. We'll try to keep it to two minutes because this is – you could probably answer this one for hours and days, because we're going to talk about data, which I think the world revolves around data, especially these days. So, I grew up in the mainframe days, right. There's one mainframe, there's Db2 database and IMS database and tape. So, you knew where your data was. You knew exactly where it was. And then we moved to client-server and then

we had data all over – PCs all over the place. Now we're in the cloud, right, and multiple clouds. So, now we have data everywhere. How do we get – you know, we just talked about a lot of compliance rules and stuff, and most of this applies to data at some level. Do we even know where our data is anymore? I mean, right now we have data distributed everyplace. We may have an API that's delivering data to customers, we may be consuming data from APIs from vendors. I mean, it's just where's our data? How hard is it now to really get our arms around this stuff?

Kayne McGladrey:
So, I'll answer that in two parts, and I'll be brief hopefully on both of them. The first part is having a policy, and when I say policy, I mean a Word document or a PDF document that's not consumable by a machine, that's been agreed to by executives that has definitions for what your data labels are. Because the last argument you want to have is what the word confidential means and to have that for a couple hours because that's a very boring conversation. It should just be straightened out, like what are your data classifications – HIPAA, PCI, whatever they happen to be. Make those words written down. Get it in front of your developers, get it in front of your application owners, get it in front of everybody who needs to attest or at least be aware of that policy. That's Part 1.

Part 2 is make sure you've got automated tooling that's going to use either machine learning, which I think is fantastic in this space to say, hey, this is also PII data, and then let's just classify this stuff automatically, because the more you can automate in this space, the easier it becomes to protect. Because if there's something I've learned about people, it's that they've got a job to do and anything that you're asking them to do in addition better be seen as worthwhile from their perspective, and most organizations have a real hard time explaining to their end users why they need to go into Windows File Explorer and say, oh, this is an applied data label at that level. It's bonkers. It's also completely unnecessary. You don't have to do that. You can automate almost all of that.

So, now that we've actually got data classification on both our structured data, and that requires talking to your database developers, your application developers and so forth. And then to your unstructured data that are on file shares and in blogs and whatnot, having a control framework that can see and do inspection of the movement of that is really important that no matter what, that data label transfers with it as it moves. If you can do that, then, assuming you've got a good SIM in place, you've actually got the ability to make some really informed decisions to say when somebody is accessing data that they should not be or, alternatively, if there's a large volume of very interesting potentially classified, sensitive, confidential, restricted insert-word-here moving out of your network or moving into an unsecure area, you can actually proactively block that, and that shuts down most of the common threats that we see these days associated with data exfiltration.

But also it lets you provide – you get to avoid accidental breaches where somebody – we had a thing here in Washington State where an employee of a company sent a spreadsheet to his spouse because his spouse was really good at Excel, and what they didn't know was that there was a whole bunch of Social Security numbers in there. All of a sudden, you've got an accidental data breach. If there had been a label, that would not have happened because the rule would have prevented it from being sent, and they would have saved themselves a whole bunch of money and training. So, I'd say that data classification, get that nailed down first, get the labeling in second, automate, it please. It's miserable work otherwise. And then just watch where it goes. And at that point, people can be working from home, they can be working from a café, they can be working from an office. That's part of the underpinning and the premise of the architectural zero trust model, which allows for that easier use of the data assuming there is classification associated with it.

Mike Kavis:
Cool. Well, I appreciate you spending some time hanging out with me today. I know you present a lot, you write a lot, you speak a lot. Where can we find all your content if we want to learn more?

Kayne McGladrey:
Let's see. Okay, so I'm @kaynemcgladrey on Twitter. That's actually kind of my primary platform. I'm also on LinkedIn, Kayne McGladrey, and if you'd like to learn more about Ascent Solutions, we are Meet Ascent, and you can find us on Twitter on @meetascent as well as on LinkedIn. Or just Google for Ascent Solutions. The company's based out of Minneapolis, Minnesota, though we are distributed across the continental United States.

Mike Kavis:
Yeah, and I saw you got snow already. I'm in Florida so we don't see any of that.

Kayne McGladrey:
Yeah, I'm in Washington State myself. I was so surprised to see snow, and I was like, oh boy, I'm so glad I don't have to go to headquarters this winter.

Mike Kavis:
Yeah, the benefits of not traveling. Well, thanks again. It was great having you. To learn more about Deloitte or read today's show notes, head over to www.deloittecloudpodcast.com. You'll find more podcasts by me and my colleague, Dave Linthicum, just by searching for Deloitte On Cloud podcast on iTunes or wherever you get your podcasts. I'm your host, Mike Kavis. If you want to contact me directly, I'm at mkavis@deloitte.com or you can find me on Twitter @madgreek65. Thanks for listening, and we'll see you next time on Architecting the Cloud.

Operator:
Thank you for listening to Architecting the Cloud, part of the On Cloud Podcast with Mike Kavis. Connect with Mike on Twitter, LinkedIn and visit the Deloitte On Cloud blog at www.deloitte.com/us/deloitte-on-cloud-blog. Be sure to rate and review the show on your favorite podcast app.