**RedZone Podcast Episode #79: Google Cloud Security: End-to-End Trust and Transparency in Your Stack – with David Cross**

Bill Murphy: … welcome you to the show today.

David Cross: Thanks, Bill. I'm really excited to be back on the show after, has it been two years now?

Bill Murphy: It's been just about two years, and it was a really fascinating conversation we originally had two years ago. Actually, I might even link up to it on the show notes. It was really fun to talk to you when you were on the other side of the fence, when you were on the Microsoft side of the fence. Now, you're on the Google side of the fence.

[00:00:30]  
David Cross:  
Yes. I hate kind of crossing over, but this is what the cloud's about, and we're all evolving. I'm a big fan of podcasts. Coming back on is a great opportunity. Certainly, I'm a regular follower of your podcast, because I always get to meet new people and things. Likewise, just like Google's constantly evolving our cloud podcast as well. So, I'd really encourage everyone to kind of join and follow.

Bill Murphy:  
[00:01:00]

[00:01:30] Yeah. One of the interesting pieces I had, interviews I had recently, was with the CIO of Experian, and actually their chief innovation officer as well. So, I kind of talked to two guys that worked pretty closely with one another in separate interviews. The CIO had a really interesting point. Of course this guy is one of the Fortune 20, 30, 50 … I mean it's up at the top. He says, "I want to be able to move all my workloads in between clouds, in between Amazon, Azure, Google." I thought, "God, what a great vision." He goes, "That's possible now." I thought, "God."

He's so far down the track, he probably thinks he's behind, and everybody else is still trying to move into the cloud securely and successfully. What do you think about that, just from a macro-vision point of view?

David Cross:

[00:02:00] Well, I think that the reality is everyone is moving to the cloud. It's not a question of if. It's a question of when. Part of it is how the clouds are evolving to meet all the needs as you evolve your applications. In some cases, it's a lift and shift. In other cases, it's really: Let's re-architect and design the next-generation web application, or to micro-services, or to containers.

[00:02:30] So, the one thing that I think we are continuing to see day after day now is that there's a lot of great on-premise applications and services, but the ability to respond to them in a rapid fashion has become more and more difficult when you're on premise. The idea is now to move the apps and data to cloud where you can actually be much faster, much more dynamic, and so that customers can benefit from the world-class operations, world-clad solutions and analysis. That's not necessarily possible in on-premise [inaudible 00:02:44] fashion today.

Bill Murphy:

[00:03:00] Yeah, it is a big challenge. One of the things that a lot of CIOs and CISOs are struggling with is … So the first generation people went to the cloud and they didn't give a shit. No pun intended. That's not really a pun, but I didn't mean to swear right there. But, they really didn't. You know? They just kind of threw their stuff up there because it was … they just did, and probably because they didn't have a lot of regulatory oversight or governance concerns or issues. I know that for a fact, because some CIOs of some high-growth companies have literally told me, "My CEO does not care. She wants it all in the cloud," or, "He wants it all in the cloud."

[00:03:30] So, now we find this generation probably the much bigger population of companies that are moving the cloud, and they're really struggling with creating the design frameworks that they had in the old paradigm, which is sort of everything gets firewalled, WINs, DNS, everything gets put behind the firewall, and now … So, that became a framework of security and operations that they could handle.

[00:04:00] Now, they're essentially trying to figure out how to firewall the cloud, and every vendor has a different way of doing it. I know that's a very kind of macro comment, but what are your thoughts from that macro piece, and then maybe we can kind of telescope into what your thoughts are, and where Google is really winning in regards to that.

David Cross:  
[00:04:30] I think that this really ties closely to what we've called our BeyondCorp model here at Google. This was one of the attractions of, when joining Google and moving to the cloud, is that moving away from just the traditional on-premise or VPN model, you know? Using your virtual private network to connect to your data center. That's just not productive in working anymore, right? We need to enforce access in mgm at the application level. And, because we're all mobile now … I think I don't even want to count the number of devices I have.

[00:05:00]

[00:05:30] I was on vacation last week, as I'm always mobile, and I'm around the world. I'm not always in one location. So, the idea is what Google has, in moving to the cloud, is really how you can actually expose your internal applications, your data, in ways where the user, the device, the code, and all the context of your location and other things, can be the context of which you have access or not. We've built out this model, and this is how it's performed at Google today, and how we're making that available through our customers with our beta of our identity-aware proxy service.

It's a completely different model because the firewalls are still in cloud, but it's not just about the traditional model of firewall out, and you VPN in. That's old-school to be honest.

Bill Murphy:  
[00:06:00] Okay, so firewall out, VPN in. I think everybody's gonna get that that has been in the technology world for a while. Essentially, you're looking at more of a proxy-based approach that, to be able to grab context. Just for those that are less technical: The context of this would be your … Well, maybe you can give us some ideas of context, because I think context is king in this world, and maybe we can drive into that a little bit, what you mean, and what Google means by context.

[00:06:30]  
David Cross:

[00:07:00]  
Absolutely. Let me start with what it means to be that. When you look at your overall data, so, when you're in an application, it becomes about data. So then, you want to know of what users are going to have access to that data, and so then you actually want strong identity and strong authentication. Then, building upon that saying, well, now that you understand the user, or that should have access to it, then what devices should they use? Should they be able to use a corporate laptop? Should they be able to use a Chromebook? Should they be able to use their phone, right? How are those proficient?

So, the context of the device is the identity of the device, but also the status of the device, right? Is it up to date? Has it been secured? Has it been provisioned and managed by the organize? That's the second part of context.

[00:07:30] The third is what location? And, in some cases, based on regulatory or other needs, it's saying that: it's one thing that, yes, I'm on premise in the corporate network, or, yes I'm connected from a home location here in Washington state, or no, I'm traveling overseas in an untrusted location or country in some cases, based on regulatory needs; and saying then, well, maybe that is a context and factor that should be played into the decision of access.

[00:08:00]

[00:08:30] Then last but not least is: what application should have access to the data? There's one thing when you look at storage in the cloud that you can say you may be running a data-processing application or machine-learning application, and that application should have access to the data. But then, there's another application that is a game application. Let's say your favorite game from Steam, should that have access to that data? Probably not. So, the context and the identity of the data itself is very, very important, and then having that policy so you can actually have a very secure location, or a secure decision in a mobile world.

Bill Murphy:

[00:09:00] So, basically, what advantages does this give versus over the VPN firewall model? Is it because of the complexity of the many different devices, that essentially you are saying that people are gonna lose if it's just … The old-fashioned model is this particular device, the firewall or the VPN would check the integrity of that device, maybe find some key or something that was resident, placed there by the company, say, "Okay, this is a device that's allowed in, and it came in," but it's just using essentially a device identifier.

What you're saying is that the goal of the Google security framework is to look at multiple different pieces of data, of which that may be one to build, to see whether that this is a trusted user, a trusted device to come in?

[00:09:30]  
David Cross:

[00:10:00]  
Yeah, absolutely. The way I like to think about it is … I think it's also important, which I was implying earlier. It's really, it's about how we think about code as an identity, at the application layer, just like we think of the user identity and the device identity. So, the way we like to think about it is, we kind of have a saying. It's: the right code running on the right machine authorized by the right identity accessing the right data at the right time.

[00:10:30] It's putting all those things together, because you may have the right identity, you may have the right machine, and the question is: Are you accessing from the right location, and from the right application itself? Because, there's one thing that, the thinking about like a VPN connection is: Yes, it's David Cross and this is his laptop, and therefore anything that's running on his machine should have access to that data. That's too broad. That's dangerous. Versus: No, this application in addition with its identity having access to the data that's specific to that application. That's another way to think about it as well.

Bill Murphy:  
[00:11:00] Yeah. That's a really interesting one, is the code as identity. So, the right code, the right machine, the right data, the right time, and the right application, so essentially that pool is … The goal from this proxy model that you referred to, and you're using the word 'BeyondCorp'. Is it called BeyondCorp, is the overall … ?

David Cross:

[00:11:30] BeyondCorp is kind of the model we've been talking about for several years now. We're now coming out. We have a beta product called the Identity-Aware Proxy that's building upon this concept, and now we can actually start enabling customers over time to actually be able to make decisions on those various contextual attributes, and when users or machines have access, and applications should have access to data.

Bill Murphy:

[00:12:00] Yeah. And, what's really interesting is that the context of this is gonna be king, and it's hard to put that together right now in the current model because of those different devices and different services running that are gathering this information, and nobody's really pulling it all together.

David Cross:

[00:12:30]

[00:13:00] Yes. The other element of it is also looking at the user identity, but it's also how did the user authenticate? You know? We all know whether it's on premise or in the cloud, phishing is still the number one entry point for attackers and risks, and it continues to this day, regardless of the location of the application or the company. And, how we move to strong authentication, that even if the user's password is stolen, without that device, without that token, without that key, that that identity is still useless; and how over time, you can actually have re-authentication, and forcing the sessions to be closed, or re-authenticated, to eliminate those risks. We have to move to that model long-term, because phishing still is the number one attack factor for all compromises and breaches.

Bill Murphy:

[00:13:30] So, what you're saying there is, from … a practical example is someone receives a phishing email, and is redirected to a site that … or, kind of in the whole attack chain, are you saying that the certs on that site typically don't exist? Or, maybe you can just kind of reverse engineer that for me, because I'm interested in if they're in the Google cloud, how would this ultimately work, that would be helpful?

David Cross:

[00:14:00] Sure. The one way to think about it is that we have, using two-factor authentication device historically has been the smart cards and certificates. And now, using OAuth and our YubiKeys is the idea is that you have to have user name and password, and also a provisioned key or device that is tied to your identity so that, not only just your username and password is also the key of your device that's already been provisioned by the company, that goes in addition to your username and password; and so that we can, even if you try to connect to something, without that key, and that piece of hardware that's in the trusted machine or device, because you can also use it with a phone through Bluetooth, or NFC, I'm sorry; then you can actually have the strong authentication.

[00:14:30] So, even if they stole my phone, even if they stole my laptop, they need all three. They need the laptop, they need the key, they need my username, they need my password. It makes the actual taking over of my identity extremely very, very difficult. So, the context of all of them.

Bill Murphy:

[00:15:00] Oh, okay. Yeah, that makes sense. Okay. That made the key for me. Basically, you're essentially putting a trusted … What's that movie where the guy talks about the part of the circle? The part of the trusted circle? It was a comedy. So, basically you have to be part of a, essentially what you articulated there was like a Triumvirat of three different keys would be together, and if that was subverted, that would be a flag.

David Cross:

[00:15:30] I think that of using the … We support this actually in both, not just the enterprise, but also the consumer space, right? It's that having anything that uses the FIDO UTF protocol in having these keys tied to your account, it's very, very powerful. So, even if you are phished and they take your password, it's not gonna be effective or usable without your key, your physical key.

Bill Murphy: That is very powerful. So, right now from the beta point of view, is that currently being offered now, or is it something that you're building into this proxy, the Identity-Aware Proxy service?

[00:16:00]  
David Cross:  
So, actually using Google cloud platform or GSuites or Google Identities with the user keys, security keys, this is available today, and so now we're tying all these other things into our Identity-Aware Proxy beta, for Google Cloud based applications, so that you can set these requirements based on your identity, and then enforcing them through our proxy.

[00:16:30]  
Bill Murphy:

[00:17:00]  
Very, very interesting. One of the things I had a question about was this … You and I had talked about the building trust in your … well, any cloud service provider. We talked about the differentiation that you have in this trusted … how this trust is being established on the Google platform. Could kind of go through that a little bit about … because I think that is a big deal for people, is: How do we trust our cloud providers? I'd love to hear how you guys are doing that.

David Cross:

[00:17:30] Absolutely. I think as we mentioned before, when customers are moving to the cloud, it's a virtual space. They do not get to see and touch everything like they do with their on-premises. The idea that we think about at Google, we run everything in the cloud. So, we want to make sure that we enable customers to have the same protection, detection, and defense capabilities that we use so our customers can have the same.

[00:18:00] Now, the way we really think about the cloud platform is, and I've talked about it before like RSA last year, right? We think about it as a nine-layer stack, right? From the hardware all the way up to the user level. We think of it's kind of like the old network layers, right? But, this one's a nine-layer. It's about the hardware, it's about how you boot the system, it's about the operating system, it's about your storage, it's about the networking, it's about the application layer, it's about the deployment, how it's deployed, it's about the operations, and it's about the users.

[00:18:30]

[00:19:00] The idea behind this is that you need to have a trusted stack all the way from the hardware to the users and applications. If you don't, then you run the risks of compromise, breach, and lack of trust in your applications that are running. So, just because you may have good controls at the application layer, if you cannot trust the actual hardware that it's running on, well, we've all read about in, name your favorite news story, of what's occurred with various agencies around the world, modifying the hardware, that the trust will not be there. Coincidentally, actually yesterday, we announced our latest blog about our tightened chip-set on the Google cloud blog, about our type and tips.

[00:19:30] It's that how we have the hardened hardware platform to ensure that we can actually have a trusted infrastructure, we have trusted boot. How we can actually ensure that when we load in the operating system and the applications is that it's come from a secure place. It has been cryptographically verified. It's based on trusted firmware, the software stack. This is the one thing that we think about strongly here at Google is that we want to ensure that we can trust the BIOS, we can trust the firmware in every device, in every component of our software stack. It's not a complete unknown, because if it is, then you can't have the trust for your data and applications.

[00:20:00]  
Bill Murphy:  
So, how do you basically ensure that the weeds are being watched? Because there's a lot of … those stacks represent a really tremendous amount of complexity, top to bottom. How do you know … for example, the key generation is happening properly? How do you know if there's a compromise? What are the mechanisms of trust that you build to verify?

David Cross:  
[00:20:30]

[00:21:00] This is something that we kind of build into our hardware or our software stack, with our hypervisor and our kernel. So, understanding that we control the keys, right? So, we control the keys of what the firmware and the microcode in our components, and so that they've been digitally signed, and that we can validate them as we boot the operating system, and put the hypervisor in place, so that we know in our overall code stack that we've modified, or that we control, to ensure that we do not bring up the system if all these signatures have not been validated.

So then, if they're not validated, or there's been a compromise, or there's a check that fails, the system will not boot. Then, we're therefore not gonna load over other guest virtual machine instances, etc., on an untrusted platform.

Bill Murphy:  
[00:21:30] So, if you were a CISO or a CIO now, what would be the … knowing what you know about Google, if you were just running a 500,000-person company as their digital leader, how would you go about testing or setting up a proof of concept? Or, what things would you turn on and start getting to know and understand on the Google platform, from a security perspective?

David Cross:  
[00:22:00]

[00:22:30] That's a good question. I think ultimately whether it's the Google platform or others, it's really is like how you actually build your threat model, understanding your risk. You understand the risk and threats to your data, and therefore then you can make sure that you will then have the right controls and policies in place so that you can validate the context of your users, your devices and applications that should have access to that data. That's the way I always like to think about things is before I put something on any application or data, saying, okay, what is my risks? Because, once you understand the risks, then you can say, "What policies do I need?" Then, based on that, what policies you need, then you apply those controls, whether it's roles, whether it's access controls, whether it's strong authentication for your users. Those type of things is the way that I like to think about this at first.

[00:23:00] What would be the number one? That's number one way I like to think about this, been moving to the cloud, or actually even deploying even on premise.

Bill Murphy:

[00:23:30]

[00:24:00] Right. So, one of the things, it's really interesting, because is … I was just in a meeting yesterday, and the CIO, she said to me, she goes, "I just want to have a way where my remote offices can patch into the cloud," she said. "But, I don't want my data going to Box, Dropbox. I don't want my data … I want it going right to my cloud storage systems." So, this is the challenge she's faced with. She wants to move to the cloud, but she hasn't figured out the right … how to govern … She wants the data going to a place where she knows it's being backed up, that it's relevant for the business, that she can grab it, because it has intellectual property associated with it. And, she's got data that's now sliding out into other cloud services. It's an interesting challenge, and it's a very practical challenge, not an easy one to solve, necessarily.

David Cross: Yes. I think this is one thing that we're looking at is, like other companies, is when this is where audit logging and things like that also come into play. When you understand of what is occurring and who has access to things and monitoring those things, then you can understand where mistakes may be occurring, where there's improper properties, or malicious behavior is going.

[00:24:30]

[00:25:00] Building upon that for Google, we're actually trying to move to a model, especially around the world, is what we call a data custodian model. This is where we're actually partnering with SAP, especially in Europe, is so that we can combine the combination of Google is a public cloud provider, and then with third-party solution providers like SAP, so that customers can have the compliance and policies that they need, specific to their environment. So, obviously you want to make sure that when you have who has access to the data, and where data is going, and who has control to that data, is this is like the two pillars, in, we say, in the data custodian model.

[00:25:30] Then, you can have the third party actually monitoring the compliance to those access controls, and long-term, how they can approve access based on the business justification needed; so that, should a cloud provider ever have access to a customer data, you want that to be transparent, and so that in the data custodian model, someone should monitor that for a customer so that they can have the confidence that their policies are being met, and the only people have access is the people that have authorized to have access to their data.

Bill Murphy:

[00:26:00]

[00:26:30] Yeah. I like the data custodian concept, because it's … I'm actually just marrying an earlier part of our conversation, because if you can actually make access validation decisions based on identifiers of software, a key, a device identifier, and you can validate who the person is, then essentially you can say that this is the rights, this person … But, we need these three elements to be in place, and now you have access to this particular data. Then, essentially by default, you'd punt access anywhere else. Like, if they're gonna move data to some place that's not a place that's been identified by the custodian framework, then that would essentially punt that … it would stop that access. Am I looking at this too simplistically, or are we essentially answering the question that she potentially has a challenge to?

David Cross:

[00:27:00] I think this is … we actually think about it in two steps, right? First is just monitoring, because I think there's two cases of where you actually have loss of automated systems. You know, machine-learning applications that should have access to the data, and this is where we have what we call the code signing and the code identity and saying that, yes, this is a trusted application. This is a trusted service, and we know this is a Google service, and we trust it. It should have access to our data, because it's performing functions on our behalf.

[00:27:30] There's this second scenario is then, let's say a support professional that is trying to help a customer to debug of something that's going wrong with their data or their application. And, this case where it's a professional then has access to the data, and that is a different scenario, because it's not based on a trusted application, it's a direct access. That's one where we say we want to have access transparency, and that it's a matter of saying, "Ah, someone had access to this data. Let's monitor that and observe that, and investigate. Oh, yes, that was support case. That's a valid access." You know, we're tying it back to the support system, and therefore there's no alert required.

[00:28:00]

[00:28:30] But then the second step longer term is then really having the controls, is to ensure that one, that you've got the right controls of not just what applications can have access. Automated, trusted applications have access to data, but also saying, "Ah, we need to let a support professional access the data," or, "We need to have a developer debug a third-party application that has access to this data, but let's improve that in giving that approval of that access," which is very, very important. So, that's kind of like the, we kind of call it our first step of transparency, or access transparency. The second step is about access controls, and so the customer can have that flexibility in confidence, it's we'll meet all of their policy requirements.

Bill Murphy:

[00:29:00] Yeah, that's great. One of the pieces you and I talk about, and I think I had asked this in our pre-conversation was: I think there's also a belief that people have that all of a sudden by giving, and this is for all of the major cloud vendors, is … but I'm interested in having this conversation with you, because I think people need to understand, who's the governor? Are customers of yours truly … do they need to still have the mentality that they're governing their own systems, even though they're basically outsourcing certain capabilities to you? Do they need to essentially have the responsibility for governing and right use? Or are you seeing people really truly being able to move their information, and all of a sudden you can just take over?

[00:29:30]  
David Cross:

[00:30:00]  
Well, when you think about the cloud, there's always gonna be share responsibilities. The idea is then how? You can actually have the best practices, the best automation in possible of the known cases of that. You don't actually have to have a manual granular touch on everything to ensure that you are protected and defended. That's one aspect of it. But, there's another element of, where in more complex enterprises, that they want much more granular control, so that they want some people to have access to the data when they're in one country, but they would not want to have those people, the same people, to have access when they're in another country, because of the risks of being mobile.

[00:30:30] So, that can only be understood and defined by the customer based on their regulatory and their specific security requirements, and so there's always gonna be a share there. But, the idea is that, how we have as many things as possible is in automated best practices format, so it's secure by default and defended by default. Then, you have the flexibility to have more granular policies when it's needed, based on your specific threats.

Bill Murphy:  
[00:31:00] Do you feel that there's ever gonna be a need to have really the public, meaning like FBI, DOD-level, the ability for cloud providers like yourselves to be able to suck in the feeds that our nation-governing services are using to protect us, in theory? Do you feel like the public companies and private companies should be able to pull that data in and use it to their advantage to secure their customers? Do you ever see that happening in the future?

[00:31:30]  
David Cross:  
Well, I probably shouldn't comment on that one, other than the overall policy is that … The one thing, like Google, like all cloud providers, I think we follow the natural regulatory and legal requirements that are provided to us. So, kind of speculating on those polices would probably be inappropriate for me as an engineer in the cloud.

Bill Murphy:  
[00:32:00] Sure. Yeah. I totally understand that. It's just one of these things that I often noodle is how we essentially marry this into one powerful ecosystem. But, what I love is how you're essentially taking, you're architecting and engineering a lot of the pieces here that in this framework of security, you've essentially architected it so that you really don't necessarily need the outside information, because you're sort of taking it into your own control, and providing these ways of mitigating risk, which I find really, really powerful.

[00:32:30] If there's one thing of the topics that we've talked about that you think that if a leader or CIO, CISO, VIP, director, someone that's in charge of their organize that they should really go dig their heels into and study and research that you feel is something that's a world-class capability that my listeners really need to understand about Google, what would that be?

[00:33:00]  
David Cross:

[00:33:30]  
You know, I still believe, and I can really credit on my mgr, Neil Provost has talked at GCP Next Conference [inaudible 00:33:10] and it's really about how when you move to the cloud, and we all will be moving to the cloud, it's really how you actually have confidence and transparency in the end-to-end stack; so that you actually have trust, and you have transparency on what is occurring in the end-to-end stack, and in the cloud. That's our nine-layer stack. If you don't have transparency and trust in that, then I think that's where your concern should come into play, because then it becomes a complete unknown in a black box, no pun intended, of your move. Then it's very difficult to threat model your risks, and apply your polices in such a model.

[00:34:00]  
Bill Murphy:  
I'm gonna put links to your RSA presentation on that. I mean that really gets into specifics. We're not really going into that of course on our show, but I'm gonna link out to that. Wouldn't you say that's a good resource for people that kind of gives the visual presentation that you gave at RSA on this?

David Cross:

[00:34:30] Absolutely, but also I'm happy to send you offline is of the more in-depth of the nine-layer stack, you know? Neil Provost, my mgr, has done it at the Google Cloud Next Conference. I think it's a nice 20-minute walkthrough of each of those layers as well.

Bill Murphy:

[00:35:00] Yeah, that's perfect, because what I want to do in the summary blog post is really just I want to give decision-makers what they need, what you feel they really need to understand about the Google model, I think that's fantastic, because you're right. At the end of the day, how can I trust something that I potentially can't trust? Really, all you can do is reverse engineer that to prove trust and prove transparency. It's really a very novel way of addressing that issue, that fear, that human fear.

David Cross: Absolutely. That's how we think about it, and that's how we're gonna continue to evolve, and that's how we're gonna continue to kind of be transparent ourselves and sharing more and more of the details of how we approach this, like our blog yesterday about the tightened chip-set. I think what you'll see hear in coming months of the things that we're doing with data custodian model with SAP.

[00:35:30]  
Bill Murphy:  
That's Titan, T-I-T-A-N, right? Titan chip? Is that how you spell that?

David Cross: Correct.

Bill Murphy: Titan ship. Last time we talked, just a little bit of personal interest here, you've been very prolific with your inventions through the year. How many patents do you have to your name right now?

David Cross:

[00:36:00] Gosh. I don't know if that's good or bad in saying that I don't know anymore. I think it's around 30, you know? I haven't been traveling the long flights as much recently, but I'm just more and more running, because I listen to these podcasts, and sometimes as a long-distance runner, when you can listen to some great security podcasts and ideas, it really gets you thinking in how to drive the next innovation in the cloud.

Bill Murphy:

[00:36:30] Well, there's a little … Are you able to remember when you're … I'm a big runner as well, and someone said to me, he goes, "You know, I can tell how productive I am by how many miles I'm running each week." So, he knows when he gets over like six miles and he's doing that multiple days, that it's actually he gets more creative. Isn't that interesting?

David Cross: Yes, exactly. The tricky thing is you gotta have in your running belt little sticky notes so as you get the ideas, you can put it down there like a napkin, and it's not forgotten.

Bill Murphy:

[00:37:00] Oh yeah, right. One of the tricks that I developed for that, David, and you might use it, is I visualize a drawer, like a dresser drawer, and I literally physically as I'm running will visualize myself writing the idea down and then shoving it in the drawer, and so then I can pull it out and my brain knows it's important, and it doesn't get lost.

David Cross: Excellent. Exactly. Sometimes, when you get these long two-hour podcasts, then you collect a lot of them.

Bill Murphy: What distance do you … Do you race, or do you just do training?

David Cross:

[00:37:30] I like always for the half marathon. You know, I can run a half marathon every weekend. It's not about the race, but you have to do a race two or three times a year just to kind of give you that motivation, you know? You gotta have just enough friction. Even though if you're just in a great rhythm, just enough friction really motivates you to get into the next level.

Bill Murphy:

[00:38:00] As we wrap up here, David, is there a take-away that you want everybody to just really understand moving forward that is sort of what you think is your central thesis that the people listening really should understand, either about something that you want to impart to them that they could take away with and something that would be really useful for them?

David Cross:

[00:38:30]

[00:39:00] The number one thing I think, I mentioned before, is when I think about your authentication, I think about strong authentication, and the fear of phishing. Really, everyone should be thinking about as a business, even if you're a small business or a consumer, is that moving to strong two-factor authentication, like UTF security keys, it's an important part of the future, because we are all going to be phished. Even those of us in the security field can be tempted and fooled. It's very sophisticated, but if you don't move to a two-factor authentication to protect your account, you will get caught. It's not a question of if, it's a question of when, and that's the one thing I always like to ask people to think about and focus on going forward.

Bill Murphy: I actually love that, and I 150% agree with you. Can you just explain though what you mean by a UTF security key, because you threw that in there and just so people, and even myself understand what you mean by that as a difference from like another security key?

David Cross:

[00:39:30] I think this is one under the FIDO kind of standard that's available. Certainly, there's a number of, like YubiKey and others that are available for the Google platform that you can use for Gmail, you can use for Google identities. Certainly, for other people, sometimes they use smart cards and USB devices with [inaudible 00:39:39] certificates. So, there's different types, and the UTF FIDO keys are the ones that Google supports with our identities in our cloud.

Bill Murphy:

[00:40:00] Oh, awesome, okay. That's great. Well, I 100% agree with you, and I think that's massive reminder for everybody. Well, this has been a real privilege and a pleasure. I really appreciate for taking the time out. I know it was a … every time I have these conversations with kind of the big five, it's always a little bit of a challenge to make sure we got the right context, but I'm so glad we got it, and get it approved. But, I'm glad we did, and it was a lot of fun.

David Cross: Absolutely. I love these, Bill. I look forward to the next one, and constantly reconnecting. I'm also looking forward to the next podcast.

Bill Murphy: Fantastic, David. Well, take care of yourself and thanks very much.

David Cross: Thank you.