Barclay Damon Live Presents *Cyber Sip*™
Season 3, Episode 16: "Zero Trust: Why You Should Act Now," With Sandeep Batta

Host: **Kevin Szczepanski**, Barclay Damon

[Kevin Szczepanski]: Sandeep Batta is lead solutions architect for IBM. As a thought leader and lead solutions architect in the Hyper Protect organization, Sandeep focuses on security and risk management for clients in the financial services, insurance, and digital asset sectors, focusing on solutions that bring the latest in cryptography and confidential computing to customer use cases. Sandeep Batta joins us now. Welcome to *Cyber Sip.*

[Sandeep Batta]: Thank you, Kevin, for the introduction. And I just want to say... begin with saying that this is me representing myself, my own views, and not necessarily IBM's views on some of the solutions that I'm going to talk about. So with that out of the way, we can get started.

[Kevin]: Let's get started.

[Sandeep]: It's a pleasure to be on the podcast.

[Kevin]: Oh, thank you. It's a pleasure to have you. And I'm excited to hear your... our discussion, particularly with respect to zero trust and Hyper Protect. Before we go any further, I do want to point out, Sandeep is going to be working with some very nice PowerPoint slides during our discussion. So for those of you that are listening alone, we're going to make this podcast interesting to you, even if you can't see the PowerPoint slides. But if you'd like to see them, I think the best way to access this episode will be through my LinkedIn page. Just click on the link there, and you'll see the visual as well as hear the audio. So with that, Sandeep, I'm going to give you a second or two to share your screen, and I'll tell our audience that we're going to begin with the question what is zero trust and why should our audience be aiming for zero trust in 2024 and soon to be 2025?

[Sandeep]: Yeah, before I start with my slides, zero trust is a concept that has been gaining ground for, I would say, about one or two years now, and especially because of so many news items that come around very often these days that things have been broken into, systems have been... I mean, we get so many things in the mail these days saying your information has been leaked, 70 million records have been compromised and all that. And more often than not, it happens because of the way information is being handled. The databases have been designed, sometimes insider attacks. Those have become really common. So the concept of zero trust is where you kind of bring all your systems into an environment where the whole environment comes together in a zero trust fashion. That means that you don't trust your insiders. You don't trust outsiders. You trust the technology. That technology should provide you that... what I call it as technical assurance that once the application is running in a technically assured platform, you are assured that none of the insider attacks or outsider attacks are going to be bothering you. And that's where the concept of zero trust comes in. And as we go into 2025, as I said, we need to be very mindful of all the advances in technology that are coming through, especially with encryption technology progressing the way it is, that quantum computing, we are going to have

a really active kind of cyber security landscape where things have to be in a zero trust environment. And so sorry for the long-winded answer, but then it requires that kind of mention, I guess.

[Kevin]: Yeah, no, I think it does. And with that, let's turn to your presentation and start with the question. It's... I think it's a perfect segue. Where are we going? We're here at the end of 2024. Where is the world going? What do we need to pay attention to?

[Sandeep]: So let me start this screen sharing. What I'm starting with is where is the world going right now. And as dynamic and accessible as any piece of content in your phone. For example, you have your shopping carts on your phone, and on sometimes you have your credit card information in a wallet on your phone. You go about using your cellphone as your payment device. More often than not, you have digital assets on your phone in terms of your cryptocurrencies or something like that. But as we go along, it's going to be even more pervasive. And in terms that governments are talking about central bank, digital currency. So you're going to have not a dollar bills, but you're going to have probably dollar tokens in a digital wallet. And so the growth of digital assets in terms of whether it's currency, whether it's any other assets that you might have, your house is probably the biggest asset you have. And it's in the form of a digital asset somewhere in an organization which holds the title, or your insurance or anything like that. So there is this estimated 16 trillion of digital assets under custody that's going to be by 2030. And the market cap of cryptocurrencies is about $2.83 trillion as of March 2034. Apple Pay, which we are all kind of... it has become kind of ubiquitous right now. Nobody pays attention if you're paying with your phone, it's about 92% of global market share.

[Kevin]: It's a tenfold increase. Then last eight years alone.

[Sandeep]: Exactly. And it's only going to grow exponentially from this point onwards as internet becomes widely available across different corners of the world. And in that context, we want to highlight that confidential computing as a market will go to about $7 billion to $8 billion by 2030. So I think it's a perfect segue to talk about confidential computing. Kevin, what do you think.

[Kevin]: Yes.

[Sandeep]: Now, given what you just... so looking at this slide deck, which is kind of animated, but for people who are listening into the podcast, what I'm trying to bring together in the slide is what kinds of digital assets that might come into the purview of confidential computing or zero trust as we talk in the regular parlance here. So it's dollar bills, your credit cards, your needs for your most important asset, your house, and everything else that come together. Your connection to your energy providers, your shopping carts, everything is going to be included. Your investments, for example, all that is going to come into the purview. And as we go into 2025 and beyond, the rate at which quantum computing capabilities are coming to the market is something very astounding. So, Kevin, should we go in to quantum computing and...

[Kevin]: Let's do that. Great. I think it's a perfect segue. And let's start with the basic question. What do we mean by "quantum computing" and why should our audience be thinking about that? And how does it figure into all of this? This interconnectivity that we're talking about...?

[Sandeep]: Right. So great question. And to kind of baseline on what we're talking about. So what we do traditionally today with all our computing devices is classical computing, where we have a flow that we go through while solving a problem. Now, I mean, the basic thing is a flow chart that we all probably understand and grow up with. Quantum computing is going to bring a whole lot of capabilities that that traditional classical computing has been unable to solve up until now, unless you have like computing capabilities that go beyond what we have today. Like, for example, some of the weather prediction models that we have using the traditional classical computing requires supercomputers and other capabilities that that that are not enough as of today. There are some like when you talk about drug manufacturing, there is a long wait time for simulations to come through and you have to go through a drug trial, probably six months, 12 months,

depending on what kind of regulatory environment you are going through. All these things. When you think about the quantum computing market, it's going to fractionalize the time that we take today with classical computing. For example, just for an example right now, the encryption that we use to protect our data, it's probably RSA encryption. And RSA encryption is as we speak, is no longer secure considering what quantum computing capabilities are going to bring in. What that means is the data that you have protected today, for example, in your bank, all your data is going to be encrypted with an RSA encryption key, and that encryption can be broken with classical computers of today. It will take some number of years to get through and break that encryption. But today, with that quantum computer, it might be possible to break that encryption in probably hours or days. So that's the kind of growth we are talking about. If you see on this slide that I'm showing right now... in 2022 and the capacity of quantum computers is measured in qubits and it's like 433 qubits in 2022 and 2023 just within a year, the... it multiplied. It's about four times right now the capability that we have in terms of work on quantum computer can bring in in terms of the number of qubits. And the next ten years, it's going to be 100 times more, something like that. So it's kind of exponential. But then this kind of capability is good for us because it's going to help us solve a lot of problems that we have today. For example, the drug simulation, drug manufacturing, some of the weather prediction models, some other prediction models in the financial markets, for example. Then there has been a lot of activity in our financial world where they are looking at the quantum computing capabilities to improve their market prediction algorithms and all that. So while on one side we have a great impact of quantum computing, the other flipside is going to be it's going to help bad actors break our encryption.

[Kevin]: Ah. So focusing on your next slide, if I could, you're... you were asking then, why is it time to act now? Why in this environment, the sort of the... in the early stages of the advances offered by quantum computing. Why now, and what is the potential impact on the data groups that we talk about most frequently health care, financial and government data?

[Sandeep]: So it's time to act now because as we know, the capabilities of quantum computing is increasing. So do the bad actors. And bad actors are just waiting in the wings right now. Any breach that you see that comes into the news that is that is probably 20 times more a breach that has happened and nobody knows about as of now. And that is the scary part. And why is it scary? Because all the data that is encrypted today with the technology that we have today, and if it is... like some organizations may not have moved into the current quantum-safe encryption technology, so they are still in the old, what they call DES encryption these or other encryptions of the '70s and '80s. Those are vulnerable, right away. And all of the bad actors who have gotten hands on encrypted data, they're just waiting in the wings for quantum computing to be available so they can unencrypt the data and then and basically run amok with it and do whatever they want to do. Ransom or I mean, we have seen in current day where hospital systems have been hacked and like ransom has been given to get back the data. So this kind of ... what we call in today's parlance as kind of a "harvest later" kind of attacks, it's like you are you are having a crop right now and you are waiting in the wings to harvest it later because you are going to have that capability in the future to kind of unencrypt that and do whatever you want, with personal data, in case of health care, it could be clinical trials data which usually last for 25 years or more. Health care records, especially in countries like Japan, where a long term like longevity goes into 100 years and all. Radiation records 100 years, the... your mortgage and the financial sector, 35 years of mortgage is very common. So anything that is hacked today, within 20 years, it's going to be it's going to be not encrypted anymore because people are waiting in the wings.

[Kevin]: So that leads me to two thoughts before we turn to your phrase, which I very much like "mitigate before migrate." Two things that I think our audience should keep in mind. The mere passage of time does not make you safe. You know, we have this... we have credit monitoring in the case of data breaches. And very often we say, all right, well, a year's worth of credit monitoring, maybe two years of credit monitoring, that'll be okay. I'm using this as an analogy, but when you turn it ... you turn that analogy towards business data, what I think you're saying, Sandeep, is, you know, the mere fact that your data hasn't been harvested or used against you after one year or two years or five years should not give you comfort if that data has been

harvested, eventually the threat actors are standing by waiting for the technology to change and eventually they will be able to de-encrypt that data. So that's one thing to keep in mind, right? The second thing that I think we should keep in mind is that we're no longer in a world in which we can say, if you have MFA, whatever that means, you're fine, or if your data is encrypted, you're fine. Increasingly, the question becomes what kind of MFA do you have? What kind of encryption you have? You as a CEO or a general counsel may be told by your in-house information technology or outside information technology or security professionals that you've got encrypt... Your data is encrypted so you're good. And the answer may be that you're not good, that the form of encryption you have is not going to last forever. And so I think it sounds to me, Sandeep, one of the things that that a business needs to do is keep... know what questions to ask and keep asking those questions because the answers change over time. What's your take on that?

[Sandeep]: I mean, the phrase "mitigate before migrate" and... stems from the fact that regulation is often behind... a couple of years behind technology and we have technological advancements in terms of encryption technology, quantum computing, and then there's something called quantum-safe computing, where you want to encrypt with algorithms, which are quantum safes. That means that even though a bad actor might have a quantum computer to break your encryption because of the quantum safety algorithms that we have been way we can use for protecting data, nobody is forcing organizations, financial institutions and healthcare companies, management companies to kind of keep up with the technological developments because that's all investment that has to go in. And then you weigh in what is the kind of investment that you put in, often the calculation comes to whether I should invest now or take the risk by ensuring my technology so that the payout for the insurance is much less than investment. And that's the kind of balance that has to be struck to mitigate before migrate....

[Kevin]: No doubt about that. So is this a good point to transition then, when we're talking about mitigation, that leads us sort of naturally into zero trust, right.

[Sandeep]: Exactly. Yeah, exactly. And that's a great segue into our main topic. I mean, we spend 10 to 15 minutes talking about why, and now the topic itself as zero trust and what we can do in the present time with the current technology base that we have available today to protect our future in terms of data security. And as we know, security of data comes in three forms. One is data addressed security data, data addressed is when data is on storage medium, for example, a hard disk or a tape drive or cloud object storage, something like that, that Amazon S3 buckets for example, so data trust. So data addressed is always encrypted, supposed to be encrypted by all kinds of regulations and all kinds of NIST-based controls that companies follow... organizations are required to follow in the financial sector and healthcare sector. The second is data in motion. So again, data is moving from one server to another, or from a server to your mobile device or something like that. That's data in motion. So all the data that flows through the wire needs to be encrypted, and DNS have been doing a fantastic job of that for years to come. Although the last... I mean, there is quite a few companies which have not moved to the latest version of TLS yet. That is kind of not surprising given the investment that goes into changing the infrastructure and all that. The third is data in... data addressed sorry data in use, sorry about the confusion. That data in use is when data is loaded into the computer. Like, for example, you want to do one plus one equals two, right? So the way it works on the server as you load one and you load another one when you do an add operation and that comes to two. Now if that one, if the two parts of the equation are encrypted, then it cannot do an add operation until you unencrypt the data. All of the other technologies like homomorphic encryption and all that which are which is out of scope for this podcast here probably in a future podcast we can talk about that. But in the traditional world we have to have data in unencrypted format, in the server's memory to be able to perform operations on that. And that is where we have seen system administrators, for example, a person who has access to the server itself in the data center, he can go and get physical access to the machine and dump that memory... dump in memory. So nothing but looking at what is happening inside the servers, the random-access memory the RAM memory. So ...and that dump of memory can reveal a lot of information as we have seen in some of our tests here. So what we need is a zero trust environment. It's something like what you see in the picture here and for viewers... for listeners,

I would say that it's like a SCIF, sensitive compartmented information facility. A SCIF is nothing but a secured compartment. You must have heard about a SCIF in TV shows like NCIS or FBI.

[Kevin]: Mmhm. The president of the United States, in during any sensitive meetings, sits in a SCIF. And if he or she is traveling, the SCIF can take on a very interesting...could be in a hotel room. It could be in a... it could be in a bedroom. It's just anything that can be secured. So when we think about this super-secure facility, that's the analogy that we should be thinking about when we're talking about zero trust?

[Sandeep]: Exactly. Exactly. So a SCIF when you is designed to go inside a SCIF and open your confidential documents or you want to do some confidential conversation, you'll go inside the SCIF and do it. And that is the zero trust environment that we are talking about and how we can bring all our sensitive applications and run them inside a SCIF kind of facility which provides zero trust environment with the technical assurance that no one else can look into what is happening inside it. So that's the zero trust environment that I want to bring along here.

[Kevin]: So when we're turning to our next slide, I think it's perfect, then, so the question I have is, all right, if we're implementing zero trust, what kinds of services and systems fall within that framework, that secure place within the organization?

[Sandeep]: Right. So usually, I mean, you have all kinds of data inside an organization's environment, so you don't want to burden yourself by putting everything inside a zero trust environment, so what we call this is the "crown jewel data." For example, for an organization that is a set of data sets which are critical to their standing in the market. Their reputation if something goes wrong, their reputation is lost and the stock price goes down, something like that. So all that kind of data, which is marked as confidential and crown jewel, those are the things that we want to identify and isolate those applications and bring them into a zero trust environment to work with them.

[Kevin]: We're talking about things—and I assume or ...for those of you that are watching, you can see it. For those of you not watching, I'll let you let you talk about these briefly, Sandeep. We're talking about critical infrastructure: financial systems and other services that need to be in that environment. Why don't we talk a little bit about that now?

[Sandeep]: So, yeah, so the first thing I want to mention, which is crown jewel is your encryption services. So everything about data is about encryption, how you store, how you're protected. And the key to encryption is encryption key... assets. So all in encryption services, for example, you want to store some data on your hard drive, you go to your key provider, which is usually called as a care master...or key management system and say, Hey, KMS, I want an encryption key to encrypt my data, and you get an encryption key based on your credentials and all that and you encrypt the data and put it away into the hard drive. Now for a threat actor, it is much easier to go after your encryption services and get that encryption key instead of spending hours and days and months trying to unencrypt or decrypt their data. So if they have the key to the encryption itself, it becomes much more easier. So instead of... like taking analogy of a house, if you have the keys to the house, you can get in. You don't have to break windows and doors to get in and do all kinds of destructive stuff. So you get the keys, you come in early and then you get access to everything that you want. Your financial systems, for example, my 401(k) or my retirement benefits, stock investments, anything of importance is under the purview of threat actors because all they want to do is disrupt and probably take away whatever you have spend years with hard work and all that. Document management systems that will include your health care records, for example, your insurance documents, your deed for your house. Now, this most important part that I keep thinking about and kind of have sleepless nights is to how to protect our critical infrastructure. Like I...

[Kevin]: ... tell us before, before we go through that, I apologize if you were going to before we talk about it, give us a good working definition when we're talking about critical infrastructure, what is it and how do we relate that concept to our organizations?

[Sandeep]: Sure. I think that deserves some time here. So our power infrastructure, for example, I mean, we have the grid... spans across the whole country and then it has it has some kind of resilience built into it, but it is not up to the mark when it comes to what threat actors can do whether it's an internal malicious actor or it could be external actors who are trying to cause disruption. And the other critical infrastructure could be our water systems, for example.

[Kevin]: Yes.

[Sandeep]: The whole city depends on a water system. Millions of people have 24/7 water supply in their house. And water system includes the purification channels that they have, How much chlorine goes into it, what kind of additives go into it. So there is a distinction between what is IT and what is OT. IT is your environment where you... information technology kind of people, they will manage the infrastructure and all that. And OT is operational technology, where you have systems which are managing your water purification plant, for example. There are different valves that are connected to Iot devices and how much chlorine goes into the water or how much other additives go into the water. They are all connected through OT systems, which are operational technology systems. Now, this is critical infrastructure because certain actors, if they get access to that, they can create havoc. And we don't want that to happen and we want to make sure all that is protected in the best way possible with the best technology that we have today. And keep up with the developments in technology so that we stay one step ahead when it comes to how things can affect us, our daily lives and all that. So very important topic there... and it keeps me keeps my mind churning all the time.

[Kevin]: So yeah no it...gets get my mind churning as well. And I think for those of us who view critical infrastructure as solely a technical term, referring to public infrastructure, I think the takeaway I'm drawing from our discussion here is that we have critical infrastructure in our country, water, power, large scale financial defense, but an organization also has its own critical infrastructure, if you will. And I think we're talking about implementing that zero trust rubric in both the public and private sectors. And it makes sense too, Sandeep, because you're dealing with, you know, where the rubber meets the road. You have smaller organizations dealing with government and critical infrastructure. So I think where we're headed is that everyone's going to have to implement zero trust, because if you don't, you may find yourself unable to be in business with those who are required to implement it.

[Sandeep]: Right. I mean, when you talk about the software build pipelines, what you mentioned about the smaller organizations, which may not have all the controls built in, but most of the software that we use today is not built by one large company. It's all sourced from different open-source platforms or smaller service providers and all that. And everybody may not have the controls that are required at a larger organization level. So the whole pipeline needs to be protected and made sure that we are following best practices and bringing zero trust to all elements of our infrastructure.

[Kevin]: So let's pivot then if we can, to the notion of crypto services for an entire enterprise. How do we think about that? And how do we implement that?

[Sandeep]: Sure. So crypto services, as we know... and the cryptography is all math, right. So you have to be able to create an encryption key, which you use to encrypt your data. And encryption keys are kind created using a random number. And if you have a random number generator in software, then it is reproducible. So you can reproduce a random number with some tries and recreate that encryption key that you use for your encryption of data and all that. So what the regulation calls for is to use hardware as security module and as you must have heard, and security literature, there are several companies and organizations who provide

what is called as HSM services, hardware security module services. And the hardware security module makes sure that you follow the latest technological developments to create encryption keys and hardware. And there are several now NIST-based controls available to follow out there. So one example that I want to give in this context is anybody who has seen "Mission Impossible," movie that Tom Cruise? I think it's "Mission Impossible 4." Tom Cruise goes into a void and he is swimming in water. He has to go inside and put in a card to kind of... get access to the whole infrastructure and all that. So similar kind of as a kind of analogy here, when it comes to exams, which is hardware security module is they are controlled by what we call as a FIPS ratings, our Federal Information Processing Standards. HSMs come in different ratings. So for example, FIPS level one, it just might be it might be say it's protected against voltage fluctuations. The FIPS level two might say, oh, it's not only protected against what is fluctuations, it can also be protected against tamper... it is tamper-proof. So anybody tries to break it, it will be protected against it. Now that the level three might be read, you know, it's protected against earthquakes and all that. So there are different levels of FIPS ratings that you can achieve for the HSM that we're talking about. And you always want to use the highest rated HSM, because that is going to be your root of trust. From a zero trust perspective. So the root of trust is how are you generate your encryption keys. And once you generate the encryption keys, how do you protect it from external access or malicious access? And that is where I bring in the slide that shows crypto services for the whole enterprise. The technology keeps moving at a very fast rate. If you have a distributor approach to it, you will have probably 25 different places in the organization that you will have to keep updating your technology every time there's a new version available or a new batch that becomes available. So in New York, make sure that you have the highest rated HSM in your organization and use that as your root of trust. And you will be assured that being the highest rated HSM, it will be protected against all the known and unknown kind of threat actors.

[Kevin]: And thinking as we... we're going to turn to the air gap for digital assets in a moment here, Sandeep, but I'm thinking there ...how would I explain to an organization why this is important? I mean, there are so many levels in which it makes sense. First, you have data of consumers, you have data of employees. You may have sensitive business data that you need to protect. Secondly, you may be doing business with counterparties that are... that will insist on a higher, more sophisticated security environment. And increasingly, that's where we're going. And if we're all not there, we're not going to get to the next step. We're not going to be able to do business with those other organizations. And the third thing I can think of, and you may have other thoughts, too, is to the extent anyone thinks today or thought yesterday that insurance was going to be a sufficient risk management tool, I think we're all going to be mistaken. I mean, insurance is something that you use after the fact. And I think what we're all learning is that the management of the threat environment in a context of zero trust is really the best way to protect your digital assets. If you're... insurance is or isn't, is an invaluable risk management tool. But if you're focused on insurance, you're really focused on reacting to a bad event after it's already happened. What we're talking about here is creating a network, creating an environment that, it may not be impervious to these threats, but it is much stronger and much better positioned to prevent these threats than your existing environment might be.

[Sandeep]: Correct. Yeah, that's right. So on this slide, just to go back a little bit, I just wanted to give an anecdote of very recent interaction that I've had. So if you see, I mentioned multi-cloud management as one of our capabilities that is shown here. So I mean with all pervasive kind of technology landscape, we use the different cloud providers to manage safer email. We have one provider for applications, we have another...and then from CIOs perspective or a CISO perspective, it becomes very difficult for organizations to keep track of what is happening to that data as it flows through all these different cloud environments. So once my data leaves my firewall, it goes into another cloud environment. Is my data protected there, in the different cloud that gets going via email or something like that, and how do I gain control over that? So for example, as my email is hacked, is it possible for me to turn off access to all data in that cloud provider instantaneously by using some kind of a multi-cloud management? So that is where a centralized approach makes the most sense because it's kind of like a red switch in your hand. And you press the red switch and access to data in a remote cloud gets disabled because you disabled the encryption key that was used to protect that data. And this is what I wanted to show. And then we can go to the edge or.

[Kevin]: Go to it. Absolutely.

[Sandeep]: Yes. Sorry about going back a bit, but I wandered...

[Kevin]: Oh, it's okay. Yeah. Okay.

[Sandeep]: Okay. So there's still airgap, as we call it, for digital assets. So as you know, digital assets are crown jewel data and it can run into trillions of dollars. And we have seen in our previous slide and we talked about it. So we want to make sure that now I mean, organizations today when they implement airgap technologies, they are manual airgaps. So what they do is there's no network connection from the inside to the outside to the inside. Any action that happens from an outside actor, it comes in as for, for example, an SD card that a person, a physical person will carry that SD card inside an organization because there is no network connectivity, and plug that SD card into a server where they can do whatever data processing needs to be done and then brings back results on the SD card to the outside. So if you see in this slide what I'm showing is on the right-hand side, there is an outside world with applications, users, and databases, and on the left-hand side I have behind the firewall an airgap which provides the kind of controls and ... boundary separation that is expected out of critical infrastructure. So this airgap analogy that we're talking about is a digital airgap that a person does not need to physically take an SD card and walk over to the other side and then wait until things are done and walk back out with the results. We're talking about using technology to our benefit and creating a digital air gap which provides the security admins and auditors a full and complete view of how the transaction is flowing from the right-hand side to the left-hand side through the servers and back out to the right-hand side. So from user to the server, processing to the outside. Now why is this required is because a person in a manual air gap who is carrying that SD card. There's nothing stopping that person from inserting that SD card into some other server to cause disruption, or make copies of that. And I mean, these are internal threat actors, right?

[Kevin]: Yes. Yes.

[Sandeep]: That would prevent against all that by kind of bringing in technology to the fore here and making use of the best way to make things up.

[Kevin]: Right. Again, we're talking about zero trust, which means we're not... we're not only distrusting those on the outside, we're distrusting those on the inside for the purposes of maximizing security and limiting our exposure.

[Sandeep]: Exactly.

[Kevin]: Good stuff. All right. So where to next?

[Sandeep]: So next what I have is build pipeline. So, I mean, when talk about build pipelines, it is all the software that goes into my application is actually run for example the digital wallet that you have on your phone or on your banking application. So any misconfiguration of that digital wallet can become very costly very quickly and all your hard-earned savings might be lost in seconds.

[Kevin]: Yes.

[Sandeep]: And we have seen this happen where a build pipeline was hacked very recently that—no mention of any names here. But we all know about two, three years ago, a small company was able to kind of introduce bugs from the build pipeline and that affected thousands of servers.

[Kevin]: Yes. Yep. So.

[Sandeep]: So? Go ahead.

[Kevin]: No. So what's the answer to that?

Sandeep: So the answer to that is what we called as a secure build services. This is where we want to make sure the build itself is done in a zero trust kind of fashion, where you bring in all your sources into a zero trust environment. And make sure the pipeline is not compromised in any way. Then it when you talk about pipeline. It is like you have a GitHub repository with all your source code, you have a team of... team from the build team. You have an auditor who want ...who should check whether the build has gone properly and all the parameters have been met. And then once the build is done, build is like converting that soft source code into executables and those developers have to be put in some kind of a repository and that repository needs to be protected again because bad actors can hack into any element of this whole pipeline, right from the source code to your digital wallet when it gets installed on your phone. So any security update that gets installed on your phone, for example. Now, every now and then—I own myself an Android phone and over the last two months I must have seen at least seven or eight updates of the phone itself.

[Kevin]: That it surprising.

[Sandeep]: That is scary for me because...

[Kevin]: Yeah, it is.

[Sandeep]: Yeah.

[Kevin]: Especially you.

[Sandeep]: [Laughs] And I'm going to paranoid about it because I know the capabilities of the security infrastructure and where are the shortfalls and all that. So I am kind of thinking about it, on how to be improve that. So any update that comes to the phone is probably a good thing because they are trying to fix some kind of a bug that has been discovered. And it's kind of scary at the same time because the more updates you are getting, the more chances for things to go wrong again. You introduce a new...

[Kevin]: Every year and... the reason is you're introducing more code and changes. And with each one there is a risk of infiltration.

[Sandeep]: Exactly. Exactly. So every new update that comes along, first of all, we have to make sure it comes from the right source. I mean, if I were installing applications which are not coming from the authentic sources, then that itself is a red flag. They want to make sure it comes from the right source. It has the right content, and it has not been infiltrated by threat actors. So that's the one that I'm talking about.

[Kevin]: All right. So, Sandeep, we've got a few minutes left. I'm going to let you take us through the balance of this really important and useful info in whatever way you think best.

[Sandeep]: Okay. So I just want to go through one slide, which is kind of very present in our current and our current day-to-day that we have... So imagine you have all the over-the-air updates coming to your car and there are several cars like that, that over-the-air updates coming. What s some doctor says all cars will turn right at 10 a.m. on so-and-so date. Imagine the I know can.

[Kevin]: It would be disastrous.

[Sandeep]: Right. Yeah. So this is an example of again, critical infrastructure, right? So what is a critical infrastructure here? If you want to identify the parts of the pipeline which are going to affect what is installed

in your car. So in your car you have updates coming and that coming from a server somewhere, it's called as the OTA update or over-the-air updates. And I mean, assuming that things might go wrong, and things will definitely go wrong, sometimes you want to make sure that you mitigate whatever might happen with whatever you have. So mitigation is going to be possible by using the current technology that this airgap that we talked about to make sure only authorized people have access to the infrastructure that sends out updates to your car's audio phones, for example, it could be anything here, wherever we are getting updates over the air. And then I should be authorized to update my own phone or my own car. No one else should be able to send out updates, which I don't approve of.

[Kevin]: Makes sense.

[Sandeep]: Those are the things which are very important. And this like, for example, the digital airgap for connective vehicles is something that is very close to my heart right now in terms of the use cases where we want to implement our technologies. So this is where I think in most of our discussion kind of culminates, in terms of zero trust and it affects our daily lives in one way or another. And we want to make sure that whatever technologies we have, we make use of that and put it in the right context and practice.

[Kevin]: That's... it's mind-boggling and critical. I agree with you. But Sandeep, let's suppose, you know, I am an individual or I'm a small/midsized business owner and I'm thinking, I understand what you're saying, but how do I get my arms around this? Where do I even start? I agree that all of these things are important, but I don't have the in-house expertise to get my arms around of these things. I can't even fully issue-spot. I, I mean, the, the risk of every vehicle turning right. For example, the auto risk. I think it's the stuff of science fiction but it's potentially very real. So this is a sort of silly question. But if you're in the elevator, it's a long one. You've got to go 50 floors. If you're in an elevator with someone in a position to make these decisions for his or her organization, what's your pitch? How do you explain it in a way that spurs action? Because this is this is not, no pun intended, a critically important investment that we're all going to be making in the next year or two or three, whether we know it or not.

[Sandeep]: Right. So in my opinion, trust is most important. You have to trust the technology that you are using every day. You have to trust partners who are bringing that technology to you, and you have to trust the regulators to kind of enforce regulations across the landscape to make sure regulations keep up with the developments in technology. And I mean, some kind of lobbying efforts are also being done to make sure that technology is taken into consideration and regulations keep up with that. So those are important things. From an individual perspective, we have to be mindful of what we're installing on our phones, make sure we authenticate or make sure that the source of where the updates are coming from, source of the applications. Think twice before you install anything on your phone. Just because it provides a service, installing an application might be really something that you would do putting a big hole in your pocket. So be very mindful of that, that those are small things that we can do from our end. But people who are designing systems, like the elevator that you mentioned, they have to be mindful of the investment that will go in in protecting and weigh that against the risk that might ensue on the larger population and the community as a whole. So that's my pitch on that.

[Kevin]: Yeah, no, that's a great point. The community and elected officials there is a role for government here. And one last question for you, Sandeep. It's about the role of a business. What role does a business have to vet technology and vet vendors that it's going to be bringing? And I, I don't know that I've done this super effectively, but I have been trying to think about and talk about vendors. We call them vendors or third parties, not as separate entities but as extensions of your business. It's like the vendor is your left arm, the technology is your right arm. It's all... you're going to be accountable ultimately for the way that technology performs. So what responsibility does an organization have to vet the vendor, vet the technology? Because of course, in many cases the that the vendor is going to have superior knowledge. So how does the business go about satisfying itself that this is a trusted vendor, trusted technology, and that the steps it's being told it should take are the appropriate ones?

[Sandeep]: Right. That great question and it's not very easy to answer or kind of put into practice, but what I have seen is increasingly vendors are trying to differentiate themselves by incorporating the regulatory standards in their build process itself. And whoever say is I don't care, technology works. I don't care about any security issues and all is kind of misinformed or kind of very loosely approaching the whole security issue. So I've seen vendors who are very mindful of getting the right certifications done. For example, the FIPs certification that I mentioned and earlier about 15, 20 minutes ago, that is something that all vendors can go through when critical infrastructure is involved. Certification will actually dissect the whole process into individual elements and look into loopholes that might exist, which could be just honest mistakes that people do sometimes while trying to get things done and nothing wrong in that. But a certification process will kind of unearth all those small little loopholes which might one day become too big to handle. And that's how I think we can mitigate at this point by making sure all our vendors go through some kind of a baseline of certification and themselves. Either it's a soft2 certification, our NIST-based controllers that are a prevalent, or ISO based controls. So there are several countries who are and trading blocs which are coming up with their own data security standards, and they are meant for protecting their own intellectual capital. And we need to respect all that and make sure we follow all that to the best possible way we can.

[Kevin]: Yeah, thanks for that. I think that's a great answer. Certification. All right. Well, before we break, I want to open it up to you. Any final thoughts, anything that you want to say that we haven't had a chance to cover?

[Sandeep]: I think we have covered a lot. But then the part where the digital airgap technology can affect the critical infrastructure that needs to deep dive sometimes and a future episode, if not me, I can bring in some of other expert to talk about on board.

[Kevin]: I love that idea.

[Sandeep]: What is being done when we have the technology, but how do we implement it right at a large scale? Sometimes the feasibility comes into the picture and then you have to weigh in the infrastructure, the investment that has to go in and what is the return on investment. All those are valid conversations to have and probably we should tackle it from a business perspective as well on how technology can best improve business results.

[Kevin]: I think that's a great idea. And will you come back some time? We can talk about the digital airgap, especially in the context of critical infrastructure.

[Sandeep]: Sure and I'll bring some partners along with me and talk business. As you can see, I'm a technologist and I some sometimes passion gets the best of me and I keep rambling about it, but then there has to be a business sector.

[Kevin]: Well, I'm in a I'm... in a somewhat unusually I'm going to end with a quote, and this is from you. "It is awful to learn about a problem with the infrastructure or service from the customer. As service providers, we must have the technology to know about issues before the customer does and bring in self-healing technology to everyday operations." And you go on to say, "I am passionate about making Hyper Protect services the platform of choice," and I think I can see why... you have a passion that I'm not saying no one else has passion, but your passion shows through. And I just I can't tell you how much I enjoyed having you come on and talk about some of these issues today. I think we could do a podcast episode about each of the slides that we discussed, but I think we made a pretty good inroad. And over the last hour or so.

[Sandeep]: Thank you so much, Kevin, for the opportunity and...

[Kevin]: I look forward to having you back and you should do more of these. You really, you explain it in a way that makes sense to people who don't live it like you do.

[Sandeep]: Thank you. Thank you the opportunity. And thank you for your entire team, too, for setting this up. I really appreciate it.

[Kevin]: Oh, thanks to you. Sandeep Batta from IBM, thank you so much for joining us. I look forward to having you back on another episode.

[Sandeep]: Sure, sure.

[Kevin]: Thanks all of you for joining us. We will be back soon, but not really soon because this is actually the end of our season three. I wouldn't ...had you told me how you have three seasons of *Cyber Sip*, I would not have believed you, but we are now at the end of season three, so we're going to take a little break. You'll see our micro content and our other publications and check out Sandeep and his creations along the way, too, will be back soon. But thanks to all of you for making this possible. I want to thank my producer, Kyla Handley, the entire Barclay Damon Live marketing team and people like Sandeep who will take, you know, an hour or more out of the day to come and talk to us. We really appreciate it. So again, Sandeep, thanks again—and thanks to all of you. We will be back soon-ish with another episode of *Cyber Sip.*

[Kevin]: The *Cyber Sip* podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, Spotify, and Google Podcasts. Like, follow, share, and continue to listen.