Barclay Damon Live Presents *Cyber Sip*™ Season 4, Episode 4: "Database Security: Risks and Safeguards," With Bob Buda

Host: **Kevin Szczepanski**, Barclay Damon

[Kevin Szczepanski]: Well, we've been waiting for this one for a long time. Bob Buda is a certified Oracle DBA. That's database administrator. And he is an expert extraordinaire on all things database design, development, administration, and security. So we're going to test Bob today a little bit about databases and a little bit about what, Bob, you and I have sort of humorously referred to as the elevator speech. So welcome, Bob Buda. It's great to have you on *Cyber Sip*.

[Bob Buda]: Thanks, Kevin. Nice to be here.

[Kevin]: So I thought it would make sense to start first in your area of expertise because then maybe you'll want to come back, because I've asked you about something that you're here to talk about. So let's start with database design and security. Now, I will confess, I had a few cases many years ago, IP cases involving database design and security. So I know a little bit about it, but I'm probably not far, much farther ahead of our average member of the audience who's thinking, yeah, I know what a database is. But I've never designed one. I've never managed one. And I certainly don't know much about how to ensure its security. So for the benefit of those of us who want to know more about database design and security, but don't know much about it now, walk us through it.

[Bob]: Okay, so I guess we'll start with what "database design" really means. When we put... we use databases for all kinds of things. They can be payroll systems or product information, product management systems, product information systems. Let's take for example, product information systems, where we'll have product formulations in the database. We'll have information about, let's imagine it's a chemical company, we'll have information about the toxicity levels of the different chemicals, health and safety information, what to do if something gets in somebody's eyes while they're handling it, what to do if the truck crashes and it's on the street and firemen have to put out a fire, what to use for that. So these are all kinds of information that we put in a database, but we can't just take all that stuff and stick it in the database, right? We have to organize it such that sometime later, when we need to get that information out, we can write programs that will understand where to get the data from. So typically they'll go into what's called tables and inside those tables there are columns. And...So "database design" means deciding what tables need to be there, what columns need to be in those tables, and what information needs to be inside of each of those columns. And then there's a bunch of other things that go along with it, for example, indexes that you need to put on different columns in order to make the queries that bring that data out, perform it... to speed them up.

[Kevin]: So I assume that Excel is one example of a database product or service. So, silly question, if I have access to Excel, what do I need my own database for? Can't I just use one of the myriad database products that are already out there?

[Bob]: So Excel is not quite a database product. It's database-like in the sense that on each Excel spreadsheet, that's kind of like a table. It's got a bunch of columns and a bunch of rows, but it's one table.

A database is a collection of tables. So database products are things more like Oracle or SQL Server or MySQL. And what they do is they give the ability to organize tables into, for example, what they call schemas. So you could group a bunch of tables together into schemas, and then you can give—and this is where security comes into it—you can give individuals access either to the entire schema that has all the tables in it or to specific tables in that schema. Or even to specific rows and columns within those tables. So that's where things like an Excel spreadsheet are very, very useful for lots of things, but not for things like organizing product information systems that have secure data, because you just can't get that granularity of security. And also, there's just a whole lot of functionality that you can...get from database systems that you wouldn't get from an Excel type of product. And again, I'm not saying they're not useful. Excel and Google Sheets and the various different types of spreadsheets that are out there are fantastic tools, and we all use them all the time.

[Kevin]: So let's say we're one of many organizations that has customized databases for our operations. Where does the concept of data security come in, Bob, and why is that so important? I assume, for example, that depending on what type of business we're talking about, we could be talking about financial information, personally identifiable information, protected health information. So how do you go about building the critical layers of security into those databases to make sure that that data is protected?

[Bob]: So before we go there, let's talk about why security is important. There are a number of things that can really hurt your business if you don't secure your data. Things like data breaches. So if you have a bunch of customer data and that customer data gets captured by hackers and put out on the dark web for sale...

[Kevin]: Yes. Mm-hmm.

[Bob]: Obviously, there's reputational damage and there's legal risk. So that's one example. Another example is competitive risk. If you have product formulation data in your database and your competitor gets a hold of your product formulations, they can make the same products that you make, obvious risk there. So those are two examples of why security matters and what it is. As far as...implementing security, there are some basic rules or some basic tenets of security that we always try to follow. And if one studies data security, what they're going to find is there's kind of a triad of principles: confidentiality, availability, and integrity. And what that essentially means is your data has to be confidential, so it's only accessible to the people that are supposed to have it. It must be available. That's kind of an obvious one, right? So if your database goes down and your applications can't get to it, you can't print product labels, you can't make formulations, you can't reach out to your customers. So availability is another key part of the security puzzle. And then integrity is that you need to know that that data is what it's supposed to be, that nobody's getting in there and changing things on you. Nobody gets in and changes a product formulation, and then you make a dangerous product or, you know, in other ways tamper with your data to make it un-useful or dangerous. So everything we do in terms of data security is about one of those three things. Probably the easiest way to think about how to get started with security is to look at the... there's various frameworks, published frameworks that are out there that outline best practices for security. Some examples are NIST, which is a government framework. They have a set of practices that one would follow in order to keep it secure. There's ISO 27001. So those are two examples. There's a few others. And essentially, they all will capture, if you take any one of those, it'll capture 95, they're 95 percent the same. And there may be some, let's say government-specific things in NIST. And there may be some commercial-specific things in ISO 27001 or the...especially the European frameworks for personal identifiable information and things like that. But if you take any one of those and implement all of the framework there, your data is going to be very, very secure. And most companies don't even approach implementing all of that, all of those frameworks, all of any of those frameworks, all of the principles in any of those frameworks.

[Kevin]: I know we're going to come to our elevator speech, and we may talk about a term that's near and dear to my heart, the risk assessment, but you mentioned NIST and ISO. And my question for you is, does it matter what framework an organization uses? Let's say you're a small- to medium-sized business. You're not

particularly regulated, although these days I think everyone is indirectly regulated. But by that, mean, if you're a vendor who's working for a regulated entity, you're probably going to have to comply with at least most of that vendor's own data security requirements. Otherwise, you're not going to be able to do business with that entity. So with that said, what are you seeing out there? How does an organization go about... an unregulated organization go about selecting one of those frameworks?

[Bob]: So it really does depend on your industry and how you're regulated... and who you do business with. You actually said it very well there, right? So if you're a regulated industry, those regulations will determine which framework you have to use. And if you're a vendor to a regulated company, the regulations they're subject to will impact you. There's more and more what they call third-party risk assessment being done. So if you're a vendor to a company that's regulated, let's say by DoD, your customer needs to follow NIST and you're going to need to, if you don't already, you're going to need to follow NIST. That's kind of coming down. It's getting lower and lower in that supply chain. Initially, it was just the prime vendors that needed to do that. And now it's being pushed down to suppliers and that's always being pushed further and further down the supply chain. So best thing to do is kind of know where your product or your service is ultimately ending up, and determine what your customer is subject to and then follow that.

[Kevin]: All right, so let's go to the lobby of a nondescript building out your way. You're from your, you're joining us today from your office in New York City, right? So you've, that's right.

[Bob]: Well, actually, I'm in New Jersey, so I'm just outside of, kind of just outside of New York City. I'm in Princeton, not too far from New York City. So.

[Kevin]: So, you've made a trip into the city and the elevator door opens and you find yourself riding the elevator of a very... the CEO of a very well-known company. And let's suppose it's a nice day, the sun is shining and that CEO turns to you and she says, what do you do? How do you steer that conversation to the first point of potential contact, where you get to know what that organization needs and you have an opportunity to decide whether you can meet that need. How does that conversation go?

[Bob]: So first I'm going to say that I've thought about this because I knew we'd be talking today. And so this is somewhat artificial. Because I've always thought that the whole "elevator pitch" idea is a great thought experiment, but not very practical in practice. Exactly. But.

[Kevin]: Yes. It is, I've never had that happen to me in 30 years. Yes, it is entirely a thought experiment.

[Bob]: But it's a really great thought experiment. So here's how I think I would try to go about doing that. I think I would ask three questions. And I would let the person I'm talking to kind of find their way. So the first question I think I would ask is, "what percentage of your annual salary would you be willing to wage that your data is totally secure?" And I would let that kind of sit for a little while. And then whatever answer I get, I would then ask the question, and this would of course depend on the nature of the business, but let's imagine that it's a chemical company like I mentioned before.

[Kevin]: Before you go to that, do you want me to answer? I'm going to be the CEO.

[Bob]: All right. OK! Great, wonderful.

[Kevin]: I'm going to be, and you know, it's an honest day. Had a good, I had an, you know, an almond croissant in the morning and had a nice cappuccino. I'm feeling pretty good after this meeting, but I get that question. What percent of my annual salary would I wage? And I would say a pretty small percentage.

[Bob]: Okay, great, wonderful. Okay, now I would ask, tomorrow morning you go into your office, and you find out that you've lost 20 percent of your product formulations because of a hardware failure and your data

wasn't backed up right. So your plant cannot make formulation today. What is the first thing that you need to do tomorrow morning?

[Kevin]: Well, I've got to get my team together, figure out what it's going to take to get back online.

[Bob]: Okay, and how long will that take?

[Kevin]: To get the team together or to get back online? I don't know how long it's going to take to get back online. My team, it's... we're going to be running around with our proverbial hair on fire. That's going to be the top priority to the exclusion of everything else.

[Bob]: And how much money will you lose per hour if you cannot make product?

[Kevin]: That depends of course on our margins, but our ability to produce product is everything. If we can't do that, we can't keep the lights on. Can't pay the employees. Can't go after new business.

[Bob]: So that's the first question I would ask you is about what happens if there's data loss. Then I would ask, now what happens if tomorrow morning, you didn't lose any data, but you found out that someone posted all of your customer data on the dark web. What are you going to need to do tomorrow?

[Kevin]: Well, I'm to have to have a conversation with all of my customers and explain to them what happened and why and what we're doing to safeguard their data going forward. But they're probably not going to have a lot of confidence in me because I'm talking to them shortly after they've learned that I couldn't do the very thing that I'm now assuring them that I can. Or worse yet, I'm not going to assure them. I'm going to say we understand this has happened. We're working the problem. We'll have an update for you shortly. But just want you to know that as of now, our systems are secure. That's not going to be a very satisfying explanation to my customers.

[Bob]: So now, how do you feel about the first question that I asked you?

[Kevin]: Well, now I've got an existential threat, right? At least arguably. So whether I can wage anything now, now I can't afford to wage anything. Now I think I've got to start from scratch. And I'm questioning the people around me. I'm questioning the people that are in charge of handling data, safeguarding data. I'm not at all convinced that I have the personnel and resources that I need to go forward.

[Bob]: So that's why I would ask those three questions. And I would encourage anyone, any business owner or executive to ask themself those three questions. Especially the ones, what does tomorrow look like? What are the specific things you would need to do if you lost data or if you had a breach? The specific, you know, they go through that full exercise. What's it really going to look like that day?

[Kevin]: Sure, and there are... we've omitted things. Obviously we're contacting counsel, we're contacting our insurer, we're drawing together our incident response team, we're running our incident response plan, we're doing all of those things, but those questions that you put to me really crystallized the big picture issues. Yes, now I've got to execute my incident response plan. I've got to go to my backups to see if I can restore my operations from backups. I'm going to do all of those things, but all I can think about is what reputational harm have I suffered with my customers and how am I going to put the genie back in the bottle? Because I know I'm not going to be able to do that. Am I going to, am I going to have customers that trust me to work with them tomorrow or next week?

[Bob]: Right, right. So, you know, I think that, you know, once someone goes through that mental exercise, what I would hope is that what their next thought is, okay, how do I increase my confidence that those things

can't happen? What do I need to, I mean, we can never be 100 percent. There's, we can never, what we need to do is we need to get to the point where we'd be willing to wager a pretty significant amount of our annual salary.

[Kevin]: Mm-hmm. Right. So how do we go from the question is then is how do we go from the CEO that says not much to the CEO says, well, a lot, maybe 80 percent, because we know that we've done all that we need to do to ensure that we have the physical, electronic, and legal safeguards in place. So can we take this a step further? The CEO is the, they've finished responding to this incident. And now they're, what one of my friends, we had him on the podcast a couple of years ago calls "post-boom." There's pre-boom, boom, and post-boom.

[Bob]: I like that. That's great. "Post-boom."

[Kevin]: So now what do we do? I come to you and say, okay, Bob, I remember having this conversation with you in an elevator. We couldn't finish it because I had to take the cell phone call that told me that everything was on fire back at the office. But I want to talk to you now because we're out of the proverbial woods, but I want to think about what steps we need to take as an organization going forward. Is this, I've got to get a CISO, I've got to implement MFA, and endpoint detection. Is there a magic bullet or set of bullets that I can load the gun with here? Or is it something more complex that I need to be thinking about a bit more holistically?

[Bob]: Well, so you absolutely have to think about it holistically. And the best way to start that is with a policy. A shocking number of businesses don't have a security policy, a data security policy. Many have security policies around their networks but pay little attention to the databases within the servers. But some don't even have a security policy at all. So let's start with a security policy. And that's an exercise that the business needs to undertake to determine what needs to be there. So clearly, there are some essential parts of the security policy, things like MFA, which are very low hanging fruit, very easy to implement, very inexpensive to implement, and very effective for stopping certain types of problems. So they're very effective at stopping hackers from getting in... into the network and even into the database to a large degree. So that's kind of a no-brainer. You have to do MFA. But it needs to go much further than that. So from a database perspective, we need to have classifications of data. So in other words, every piece of data in the database needs to be classified as whether it's sensitive or not. We can't just assume everything is sensitive because if you lock everything up, nobody can do their job. So there are some things that are sensitive, there are some things that are not, and they need to be treated differently. So. So, and in order to effectively treat data differently, they need to be classified. So, we have to have sensitive data and non-sensitive data. We need to determine how much we need to protect that sensitive data. Does it need to be masked when viewed by internal users? You know, are there only certain users that can see the real data or are all internal users okay to see it? What about data that customers see? How much of that can be exposed, how much of the data can be exposed to the customer. So all that kind of stuff should be laid out in the security policy. And then there is more technical things in the security policy, like, for database users, what kind of password protections are there? How often do they need to change their passwords? How strong the passwords need to be? All those kinds of things. All should be laid out in the policy because if you don't have the policy written, you don't know what you're measuring against. That's the kind of thing number one is have the policy, then determine everything you need to do to implement that policy. And I'm going to skip all that because the most important thing, it's table stakes to have all those things. You need to have those things.

[Kevin]: Mm-hmm. Right. Agreed.

[Bob]: And many companies get that far. They do have a policy, they do put in processes to manage their data, and they put in processes to back up their data and to have disaster recovery in place and things like that. I would say the next most important thing for if we're talking to lots of companies out there is testing.

Testing DR, know, testing disaster recovery, testing backups, and testing security is not done enough and it needs to be done a lot more. And it's absolutely essential. I can't tell you how many times I have seen backup environments—since we're a database team, that we think in terms of backups and disaster recovery from a database perspective. And frequently, we find new customers... First thing we do when we come into a customer site is we do an assessment of their disaster recovery, of their backups, of their whole configuration and all that. Very frequently we find that they don't really have the backups they think they have. Meaning, backups were configured at one point and then stuff changed, and it was never reconfigured. So they have backups, and they run every week, but if they have to restore, they're not going to get all their data back. And that's why the example I gave in the elevator, was what happens if you lose 20 percent of your data? Because it's the 20 percent that was archived and it's no longer on the main drive and it doesn't get backed up anymore. And we've actually seen that exact thing happen. So testing recovery is really, really essential and it's a lot of work and it takes staff time, and it takes a dedicated team or individual to do that. But if you don't do it, you really can't wager 80 percent of your income that your data is protected because you don't know it unless you test it. So that's, I would say that's, if you want to get to the place where you could be totally comfortable that you can wager a lot of your money, test. At least semi-annually. If you have the luxury, quarterly. And if you have nuclear secrets and you're running something that can cause harm, monthly. It all depends on how critical things are. Everything is not nuclear secrets. So there's room to assume a little bit of risk depending on what you're doing. And of course, you need to think about that because it's expensive to do this stuff very, very, very rigorously. So there's a sliding scale there and you need to know what your tolerances are. Of course, I didn't mention this earlier, but as anyone goes through this exercise of setting up disaster recovery or backups, one of the things a team like ours would do when we talk to you about it or even setting up your security policy is we would talk about your tolerances. What is your tolerance for downtime? What is your tolerance for data loss? So it may be okay to lose half a day of data because your volume may be low enough that, and you might keep stuff on paper so you can put it back in. And if you can save $50,000 a year by accepting a half a day data loss, it may be worth doing that for you. So you do need to identify what your tolerances are for pain in those various ways. Pain of losing data, pain of being down. There's really zero tolerance. There should be zero tolerance for data breaches. I mean, unless you really don't do much, there needs to be zero tolerance for data breaches and things like ransomware. That's a really insidious thing that can cripple your company if you're not careful enough to have offsite backups that are firewalled from your own infrastructure. Because any company—and a lot of times people think, well, we're too small, they'll never look at us wrong.

[Kevin]: No, that's not true.

[Bob]: They look at everybody.

[Kevin]: And those are the companies that fare worst, Bob, because they tend to have fewer safeguards in place. So when we encounter those companies in data breach or ransomware scenarios there, they don't have insurance, they don't have backups, and it is an existential risk because they literally cannot do business for hours, days, weeks, sometimes even more.

[Bob]: Correct.

[Kevin]: We've seen that.

[Bob]: And sometimes they go out of business. Sometimes they can't survive it. So it is an existential risk.

[Kevin]: Yes. So I don't mean to put you on the spot, but we talked about data security policy. We talked about testing. What's next? We've got those elements in place. Is that everything? Are we good? Or should we be thinking about something else?

[Bob]: Well so... maintenance of policies and of data is really critical. So let's take those two separately. Let's talk about maintenance of policies. When a company is small, let's say you have a company that starts out, they've got $10 million in revenue, they've got a few hundred customers. They have a certain security policy. That same security policy may not serve them well when they have $500 million in revenue and thousands of customers and customers in other places. When they started out, they may have just been US-based. Now they're Europe-based. Now the security policy has to factor in European controls. So the policies need to be revisited on a regular basis. So that's maintenance of policies. So they need to be revisited, tested. And I don't mean the kind of testing I was talking about before but testing those policies. Run them by people other than those who made them.

[Kevin]: So for example, and tell me if this example makes sense, if you have an incident response plan, sort of picking the low hanging fruit, you should be testing that IRP with something called a tabletop exercise.

[Bob]: Yes. Absolutely.

[Kevin]: And there are different tabletops. They're not all created equally. Sometimes it's sufficient or the company can't afford much more than a third-party led discussion. Where there may be a PowerPoint, we may just be running it informally. But I think the most effective, if you can afford it, is a real-time simulation, where you have all of the stakeholders in the room and you have a trusted third party that is literally running a disaster to see whether and how you can respond.

[Bob]: I really agree with that because the third party has no incentive to hide anything, and no incentive to play down anything. I think that if it's all done internally, first of all, everybody's busy and everybody has other priorities, and they just want to get out of there. They want to get this thing done and get out of there. So there's a lot of incentive to just cut corners, skip little things, and the third party won't let that happen. So I totally agree with you. I think a trusted third party is essential to one of those kind of tabletop exercises. And so that goes along with the testing that I was talking about. I don't think you need to do the tabletop exercise every quarter. I mean, the full-blown disaster every quarter.

[Kevin]: Agreed. Agreed.

[Bob]: I think every quarter should be the technical aspects of your disaster recovery. Make sure your backups are working. Make sure you can recover to the environment that you have or over to your standby site, that kind of stuff. And I think that a trusted third party there again helps because if it doesn't work, that's going to be recorded. It's going to be, you know, it's that third party is going to be under the gun to make it work. And if it's an internal resource, they're under the gun to get back to their other job. And so there's a different set of incentives there. So yeah, I think a third party is a valuable addition really to all of those types of tests.

[Kevin]: Agreed. And there are many out there. I interrupted you talking about testing and tabletops, which is important. You left off with your discussion of maintenance of policies and data. We talked about maintenance of policies. Talk to us a little bit about maintenance of the data itself.

[Bob]: Okay, so now I'm going to break the maintenance of the data into two pieces. So there's the maintenance of the database. So the database, as we discussed in the beginning of our conversation, are things like Oracle and SQL Server. They're collections of data, structured and made accessible to different people. There's all kinds of things that need to be done to ensure that they continue to operate and that the data doesn't get corrupted or that they don't fill up with space and are unable to continue operating. So there's maintenance activities that need to take place on a regular basis. With our customers, we do that on a weekly basis. And it means going in there, looking at all of the indicators that tell you whether the database is healthy or not, that tell you if you're filling up, there are things called archive logs that record data as changes are being made. There are audit logs. There's all kinds of things that can go wrong if we don't pay attention to

them. There's also performance issues that take place as you add data. Things can slow down unless indexes are maintained. So there's database maintenance. And then there's data maintenance. So data maintenance is things like ensuring that the data is clean and accurate. And it's things like archiving old data, ensuring that the data lifecycle is being maintained. So some companies have to keep data for a certain amount of time, but they don't want to keep it in their main database because it takes up a lot of space and that's expensive because you're on fast storage. So you take some of that and you put it somewhere else. You may have to take that offsite for compliance reasons. So that's data maintenance. So those two things need to be done on an ongoing, regular basis. In our discussion that we had a few weeks ago, we touched on this a little bit, but more and more data is going to be used for the purposes of training and using AI, artificial intelligence and machine learning models.

[Kevin]: Right.

[Bob]: And when that starts happening, data maintenance is going to become more important because in addition to making sure the data is clean, we're going to have to make sure that the data is, I'll say, presented to the AI models properly.

[Kevin]: Right.

[Bob]: We need to make sure that the AI models will know what it's getting when we're sending in that data. And that means things like applying labels or metadata to the data. So that's a newer task in data maintenance. And so those are the two kinds of maintenance. So the maintenance of the policies and the procedures, the maintenance of the databases themselves, and then the maintenance of the data. I think those are really three very critical maintenance pieces.

[Kevin]: How common is the AI issue in your world these days, Bob? People are focused on OpenAI, ChatGPT, and some of the other well-known outside large language models, but many businesses have already done this, and I think many will, maybe in my world, the world of the law firm, will continue migrating to their own private large language models to facilitate in-house work without supplying confidential or protected data to an open source. How common is that? And where do you see that heading? I'd love to get your thoughts on that.

[Bob]: So I was having a conversation about this with a colleague yesterday, and he used a great term. Most customers that we come across now are in a phase that he called "AI-curious," meaning what they're really trying to do is figure out the use cases. And the one use case that everybody thinks about now is chatbots. And a lot of them already have that.

[Kevin]: Right.

[Bob]: But there's a lot more that can be done with machine learning and with AI. Bigger companies and high-tech companies have been using machine learning for a long time. But the advent of large language models like ChatGPT and Gemini and these other things have, I think, made... So large language models are a type of machine learning model. And the advent of large language models, I think have made machine learning accessible to the rest of us now. And so a lot of companies are really in the early stages of thinking about...they have all this data, have tons of different kinds of data in all different databases and in... unstructured data, lots and lots of PDF files and spreadsheets and all this kind of stuff, images. What can they do with it? So, you know, I wouldn't say that there's a common use case that I've seen. It's really... right now for my customer set, just the beginning of thinking about how to, what can we get out of this? What can we do with it? And, you know, once they figure out what they can do with it, the next challenge will be how to do it and picking the tool sets to do that. There are, as you mentioned, there are some main models out there that everybody knows about, but there are probably thousands of other lesser-known models in the open-source world. So

there's going to be a lot of work to be done in choosing models that make sense for whatever the use case is. And then in building pipelines to get your data from where it is now into either a vector database or some other form where you can use it to either train the model that you choose or to use it to do inference on...when you're pulling the data out of the model. And there's going to be just a whole lot of technical plumbing to be done once the use case is determined.

[Kevin]: It sounds like it. So if you're "AI-curious," as you said, you're a company that's AI-curious, you've got to work to build that use case. And then you move from there to the technology to actualize that use case. And then I suppose you've got to get some history. You've got to see how it works. You've got to tinker with it. And only in that actual experience phase are you going to know whether it works or not, if it doesn't work perfectly, how you're going to continuously and incrementally improve so that in a year's time, three years' time, you've built that AI into your business and you actually, you're experiencing that return on investment.

[Bob]: I think that the real key for business leaders is to choose use cases that have value, even if it wasn't AI. I think that we all have a tendency to want to use new technology. All of our colleagues are using it. If I don't introduce it into my business, I'm going to be seen as...

[Kevin]: ... a troglodyte.

[Bob]: Yes! Thank you. And I think that we need to really fight that and ensure that the use cases we choose are things that, even if it wasn't AI producing the output, would still be useful to our company, if that makes sense. Take the AI out of the equation until you know the use case.

[Kevin]: Yes. Right. So in other words, I don't have to think of something completely new. I should be thinking about the various products, in case of a law firm, the services that I deliver today. Those are important services. So how can I use AI to make the delivery of those services more efficient?

[Bob]: Right. I would actually think of it differently. I would say, if I had no constraints at all, how could I improve my service? And then determine what those things are, and then say, can AI help me do that?

[Kevin]: Got it. Mm-hmm.

Or how can AI help me do that? Rather than thinking, how can I use AI to do that? What can AI help me to do? Approach it from the other way and say, if I could do anything I want, what would I do? And some of those things will still be impossible, but some of those may be facilitated by the new tools that we have with AI.

[Kevin]: Yeah, I've got you. So the point is not to start with the question, how can I use AI? Start with the question, what do I really need to accomplish? And can AI serve that objective? And if the answer is no, then the answer is no. You don't need it.

[Bob]: Exactly. Then the answer is no. And that surely there will be things that AI can help with. But I think finding them from a business and a customer perspective is a more certain way of landing on the use cases that will add value than going the other direction.

[Kevin]: Love that. I love that. All right. Bob, we've got, I want to be mindful of your time. We just got a few minutes left. Do you, is... before we transition, we talked about data security policy, testing, maintenance of policies and data. What, if anything else is on that list? If you've got a little extra time to talk to that, that CEO.

[Bob]: So the main thing—I use an analogy all the time because I think it's so important, I'm going to use it again.

[Kevin]: Oh, love it.

[Bob]: Many companies think when they think in terms of security, they think of the perimeter. So they think a lot about securing the perimeter and they don't think about going a step further and securing things at the database level. They do cursory security at the database level, but they don't really, they don't pay a lot of attention to it. And the analogy that I like to use for that is, you know, someone who...a family goes on vacation, and they have a safe in their bedroom and they put all of their jewels and their stock bonds and all these things, their stock certificates into that safe. And before they leave, they lock up all their windows and they put on their alarm system, but they leave the safe door open because they've secured the perimeter. They've put their alarm system on. So why do I need to close the safe? That's what a lot of companies are doing. All of their jewels, their product information, their formulations, their most important things, they're concentrated in that database. But we don't secure that database any better than we secure the stuff around it. And that makes no sense. Especially because there are lots of tools that the database providers, the database vendors provide that enable you to really lock that down Back to your original question about Microsoft Excel, that's an example of where an actual database product gives you more functionality. It gives you the ability to secure that data better than if you just put it in a bunch of spreadsheets. So that's, know, I'd want to leave people with that vision. You wouldn't, if you have a safe in your house, you wouldn't leave that safe door open when you go on vacation, even though you've closed all your windows and locked all your doors. You would make sure that safe is closed, because that's where the real stuff is.

[Kevin]: Right. It's funny when you were saying before you got to that, drew a big rectangle with three smaller squares inside because I wanted to ask you about that. And I'm grateful that you brought it up. Of course, it leads to a question that I may have to have you back to talk about, which is zero trust. Not only ...to me, at least analytically, the next step from perimeter security to data security is, all right, what about security from insider threats? The assumption is that the only threats are going to come from outside the perimeter, but that's not always the case. And it's not always the case that we're talking about malicious insider threats, right? We could be talking about failure to log off or clicking on a link. There are all sorts of insider threats and that has led to the concept of zero trust. And I know we've only got a couple of minutes left, but I want to... will you come back and talk to us about zero trust sometime? I'd love to have that conversation.

[Bob]: I'd love to. I think that would be a fun conversation. But what I'll say about that is whether it's internal or external threats, what zero trust does is it increases the granularity that you have when controlling access to the data. So this... it ties into the data classification questions that we talked about. It ties into everything. It ties into treating the database as a more special thing than things outside the database. It ties into all of that. Yeah, I mean, that could be a whole 'nother conversation.

[Kevin]: I would love to have you back to talk about that.

[Bob]: And I think that's an important subject. Not a lot of people are implementing it. It's hard to implement. There's a lot of work that goes into it. And to tie everything together here, you made a point of talking about maintenance before and about maintaining the policies, right? So when you have zero trust, there's a lot of maintenance going on because it's all dynamic rules that you put in place that can change. And you need to make sure those rules are always right when you use zero trust. So love to come back and talk more about that. But that's a great conversation to have.

[Kevin]: And this has been a great conversation. And I just want to thank you for joining us, Bob. We've had a couple of nice conversations, one of which on *Cyber Sip*. I hope to have many more. And I think there's no better place to leave it than right where we are now. And you're committed to coming back. But on a serious note, love to have you back anytime. We can talk about zero trust. We can talk about my odd passion about risk assessments, because I think that's a...

[Bob]: I'd love to talk about that.

[Kevin]: I think it's important and I think what we're seeing is it used to be even as recently as two years ago, smaller, mid-sized businesses could essentially ignore these things because the answer always was, well, you're not publicly traded or regulated you don't have to worry about this. If you're doing business with a regulated entity or an entity that is subject to any of these more stringent requirements, you're going to have to comply as well because you as a vendor are an extension of that entity. And if they don't meet those requirements either directly or through you, at the very least they're going to ask the question, do we really want to go with this vendor or do we need to safeguard ourselves by going with a vendor that can comply with these more stringent requirements?

[Bob]: Yeah, that's 100 percent right. We, as a service provider to financial companies, we have to comply with the security regulations that they have to comply with. And so we get pages and pages of third-party risk assessments that we have to complete all the time. And we're a very small company. Yeah, size does not get you out. It's not a "get out of jail free card." You have to be just as rigorous with security as if you're GM.

[Kevin]: Well, that's an even better place to leave it. Bob Buda, thank you so much for joining us on *Cyber Sip*.

[Bob]: Thanks Kevin, thanks for having me.

[Kevin]: My pleasure, and thanks to all of you. We will be back soon with another episode.

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