Di **[00:00:57]**: Tony, maybe we could spend a little time now talking about some of the details of your project management?

[00:01:04]

First of all, may I ask – because this is always a concern for your fellow practitioners across the country – where did you find the resources to find this effort? Can you talk to that?

Tony: That's a very good question, and I have some words of wisdom about that from the Hard Knocks School over here. The first thing I tried was I tried to go out and find funding for identity. I tried to find it based on a number of effective use cases, and that didn't work at all. Suggestion: Don't go there.

Di: You knocked, and no one opened the door.

Tony: No one would open the door, no matter what. So the next thing I did was I looked at the current business process and used such simple, accepted metrics as the number of password resets, the amount of time it took for someone to log in.

[00:01:58]

I did a survey on the number of systems and credentials that each staff member was keeping track of or trying to keep track of, the number of systems that they went into. I got very analyst oriented, analytic about the user base, and then I took those numbers back and I said, "Great, there are industry standard numbers about the cost of a password reset, about the amount of time a help desk takes." So I took those industry standard costs and our own county data, and I put that together and presented a case for some initial seed funding to get that going based on that ROI [return on investment], which turns out to be very short, and no one could believe it, because the cost of password resets is so high.

Di: Really?

Tony: Yeah.

John: What was the average number of credentials that people have to keep track of?

Tony: In our county, we had people who had 15 credentials that they would keep track of. They had their normal log in. They might

have had their payroll log in and four or five different other systems, and it just adds up when you started really talking to them.

[00:03:03]

Initially everybody says, "Well, I've got way too many," but what we did was we listed them all out.

John: Did you get any honesty from them about really how many different passwords they have for those 15 systems?

Tony: As a security officer, I got information that was a little alarming about the number and simplicity of the passwords they would be using. Typically they would say, "Well, I make them all the same every month." Or it's 1-2-3, and then it becomes 1-2-3-4, and then it becomes 1-2-3-4-5. Various answers like that. So the password complexity was certainly not something they were into. Security wasn't at the top of their list. It was all about the efficiencies.

So looking at it as moving toward a single sign on solution – everybody was on board with that.

Di: So that gave you some seed money to start developing the proof of concept.

[00:04:00]

When you went out into the open source or commercial software market, Tony, what did you find that would meet your needs?

Tony: We found over 35 different products or vendors that initially looked like they'd meet our need. Then as we narrowed it down to having a portal, having a portal that did user provisioning, having a portal that did entitlement management or access, and then did the access control, and did all of those functions – pretty soon that matrix came down to a much smaller number. There were only four or five who would do it. Then we looked at it in terms of the simplicity, and there were some solutions where we could add a federation service, etcetera, but we'd be adding 12 servers.

Again, in Orange County – different than some of the users watching this might be – again, we have 37 different agencies, each having their own entities and their own active directories.

[00:05:00]

So in our case, if we had to populate different identity boxes in each of those, the cost would get alarming.

Di: Very quickly.

Tony: Plus our vision is to be able to support folks who are not agencies of the county: those independent attorneys, those clinics. So I didn't want to have to place a box – again, I'm trying to be very careful not to mention any manufacturers – but to place one of those identity boxes out at those locations as part of the architecture. So that narrowed it even further.

Then we looked at licensing costs, and the challenge is that many of the vendors were expensive in their first-time license purchase and then in their ongoing renewal. So we ended up using a solution which is from a smaller company which does an enterprise version of their open source community version. So their licensing model has got a lot more flexibility in it, because we're paying basically for a support contract, not for licensing.

[00:06:00]

The feature enhancements that we contribute go back into the general pool of features, which most of the larger commercial companies we talked with, that's really what they do anyway. They work with a custom implementation for one customer, and then they put it back into their normal product. They just don't call it the GNU standard open source licensing model. They call it proprietary intellectual property. But either way, you pay more for it each time. In our case, our licensing is very reasonable.

Di: When you were whittling down this list of potential providers, were the national standards important to you? Were you looking for SAML [Security Assertion Markup Language]? Were you looking for –

John: The industry standards.

Tony: Yeah, we definitely had on our checklist that it had to have Active Directory, LDAP [Lightweight Directory Access Protocol], SAML, it had to have web services. It had to have standard encryption.

[00:07:00]

All of those things were definitely features, because the success of the project is integrating with new applications, yes, but more importantly, the success of our project was about integrating with legacy applications. We wanted that portal to be your single portal into everything going on. And so that meant it had to have all those connector supports. And of course, the interface had to be customized for our needs, so we needed something that had a flexible UI [user interface] structure. Some of the vendors we talked to, basically they had their standard product, and they weren't willing to change it.

In this case, our self-service portal has become more of – the vendor offers a very similar self-service portal as their standard product now. Every time we put an enhancement in, as I said, part of the open source license, as you know, is it goes back into the normal product features.

Di: Well, thank you for contributing to the evolution of the product, Tony. That's great. Have you been able to gather some data about what the payback has been, what the return on investment has been?

[00:08:04]

Or maybe it's a little too early?

Tony: It's a little early to be posting the numbers. We have some preliminary numbers, and it's very encouraging. We're seeing the users in our healthcare organization, their feedback to us is, "Why didn't we have this before?" which is always a good thing.

John: It's positive feedback.

Tony: But in terms of actual dollars and cents ROIs, I think we're still a little early. I'd like to get it rolled out to more agencies on a larger basis, because, again, remembering our portal concept, if I only give you launching one application, even if it's a payroll application or something simple that you do, I really want to – the return on this is to be able to have five applications on a single log in. There you'll see the user satisfaction go up, and the dollars and cents payback will be there.

[00:08:57]

Di: So you had described a couple of categories of data to make your business case initially – password resets, how long does it take people to log in, how many credentials are people really having to manage. Are you imagining that those will be the same kinds of data that you'll collect for your return on investment?

Tony: Yeah.

Di: Do you see any other benefits flowing? Enhanced security?

Tony: The enhanced security, and again, that's a harder one to measure.

Di: It is.

Tony: The number of systems that you get data from is another metric. And it's going to be one in which they said, "Gee, I previously didn't exchange data with the courts. I previously couldn't get data from social services," so it's really the number of use cases that you're able to use now that you couldn't before, the number of data exchanges you have today.

Again, because one of the values of our identity provided solution is to integrate to a variety of databases, including the courts' databases, is very critical here because they have not only the juvenile, but they have adult and the calendar, etcetera.

[00:10:05]

Even in the courts thing, we anticipate that the win-win will be here's seven databases that I get valuable information about that I didn't even know existed before via the one portal. So again, that's not a metric that we were able to compare before because it was zero. But we know that as that goes up, the value to the end user goes up.

John: There's another opportunity that occurs, and that is: I may have access to the seven systems, but the time to log on and query each of those seven systems and then write down the information to compile my bail deviation report, I don't have a lot of time to give a recommendation whether they should be released out on bail deviation or not. This way, you can start building in the background queries to all seven sources compiling that as a response.

[00:11:00]

Then, the consumer can see the consolidated view all at one time as opposed to what he's had to do traditionally is go from system to system and log in and log out.

Tony: So really that time to data is a metric that you'd like to say, "Time to data is very short. Whereas before, I didn't even know the data existed, and I couldn't get there." That's really going to be part of – so again, I'm holding off on doing some of that final report because I want to get the bigger picture, show the bigger win.

When we initially started, our success criteria was basically driven off of the number of users, very simple, easy to go; the number of log ins, meaning how often are they using it or a percentage of adoption; the number of credentials that someone felt they had to have, so we're going back to the same people and asking the same questions in that case. We really see that that'll be a win-win.

Di: What are your thoughts about the long term sustainability of OCID?

[00:12:02]

Understanding that you had some funding to prove the concept, understanding that you believe you've got positive ROI, how do you as a county enterprise imagine supporting this for the long haul?

Tony: Our current activities are based on that proof of concept that we got initial funding for. A lot of times, everyone says it's hard to get money and it's hard to get proof of concept money, but I think proof of concept money is easier in some ways to get than the sustaining money because they see it and they say, "Well, now just feed it into some other rate." That's what we're going through right now.

We're looking into the next year and saying, "Okay, is this part of a security rate, or is this part of some other rate?" Now the advantage we have is that because we're leveraging the open source environment, we have lower costs, so adding it to the rate looks as though it's about – what did we say? It was like $2.00 a month for a user.

[00:13:01]

Now, we haven't finished all the rate numbers, so that's just off the cuff. But if $2.00 there gets me the whole month and I get access to all the data and I don't have to remember all the passwords, there is some value there that you could argue.

But we also think that there should be some other sources of funding that we're going to try and find, because we are enabling other kinds of access where the agencies will have reduced staffing. So if I can make your staff more effective in social services because now you don't have that three-day delay in getting access to it. But the problem we're faced with is that it's difficult to convince other agencies who are tight on money that just because it's more efficient for them that they should give us some sort of funding for that.

Di: It is difficult. I understand what you're saying. But the use case that you described was that someone is standing at a copier somewhere, scanning documents to respond to a request somewhere. And they don't have to do that anymore.

[00:14:08]

Tony: The good news for us is that part of what we did here in the upfront was we spent a lot of time visiting the end users, working with them to find out what is it they do today and documenting that. So when we come back and we say, "We've changed your business process. You're not at the Xerox machine anymore." Or, "It's not taking you three days to wait," that we should be able to come back and show that to the agency as an improvement. Not necessarily will we get the funding, but it's been beneficial to have done that in-the-trench work.

John: I think an important maintenance component is the resources that are being made available, those resources undergo maintenance changes, and they undergo database changes, and that means the portal's interface, and the scope of elements may change over time, and that needs to be maintained.

[00:15:04]

So interfaces become a piece of work, as well, that in the absence of those interfaces or the old interfaces, it was all done at the application level. Now you have to coordinate when you're going to change something.

Tony: One of the sources of funding going forward needs to be that when you register your data structure into the identity manager, there's an integration fee. Although it might be as simple as a SAML or an AD [Active Directory] connector, we're going to charge an integration fee because that project was funded to get integration. We're hoping that we can get a small piece of your large pie to improve your project.

John: An ongoing fee or a one-time fee?

Tony: It's probably going to be a one-time integration fee. So we're still looking at how do you bill this back, either by user or by database by which you're acting as a front end for? Again, you'd like that to be an ongoing, but this is all new and novel.

[00:16:03]

There seems to be enough money to be able to buy the iPads, but when it comes to the identity piece, it's questionable.

Di: Anything else you'd like to bring forward about funding? John, do you have anything that you'd like to bring forward from your experience now with your Los Angeles hat on?

John: I think that our departments – our larger departments, anyway – they have the resources to stand up an identity provider for their agencies, and they're pretty much going to absorb that based on the business benefits of being able to then use that identity to access – again, most of our communications or information sharing is between the justice partners themselves. If I was going to take all the justice information sharing, I'm going to say over 90 percent of it is within the local jurisdiction.

[00:17:05]

What goes vertically – there are interfaces there, but they're not near the volume that you look at locally.

So enabling their applications to accept the credentials from the other justice agencies and vice versa, they see the real benefit of that. And so I see it being absorbed within those various business units. So I don't face the same funding challenge, I don't think, that we're not running a centralized portal and doing the integration to all those sources. They have the technical expertise that they follow the standard for how to enable the service and how

to set up their identity provider and have agreed that we will work collectively on the common attributes that we share.

[00:18:02]

Tony: And you've got some very large agencies, so that's a challenge too.

John: Yeah, we do. Sure.

Tony: You'd like really to – instead of having each agency stand up their own, you'd like to do what we're doing, I think, is a single one just because it's simpler to have one than many that you have to keep up to date and integrate, etcetera. But again, in some of those larger agencies, it's harder to convince them to all play together.

John: That's a given, yes. They could play together on the standards platform, but in terms of – law enforcement has its own data centers separate from the county's data center, and so does the court, so we have at least three data centers in L.A. County, major data centers.

Tony: On the security side, we really looked at this identity as an emerging issue, but over the last five years, we kept thinking, "Well, maybe the state will do something." So now we've just said, "Well, it has to get done, and it'll get done at the lower level." It may be that in ten years towards your vision to the future that these identity providers will exist at a state or a federal level, but I don't know.

[00:19:05]

John: Yes. NASCIO [National Association of State Chief Information Officers] has goals and visions along those lines of having state-provisioned identity management services, but it hasn't been realized yet. It's a goal, and it's being discussed, but it's not there.

Di: So this is a little bit of a tangent, but as you're looking out, John, across the nation at some of these identity provider implementations that you're aware of, is Orange County unique in its inclusion of private parties who do business with government, but are not employees subject to hiring and firing by the government? Is that unique in Orange County, or are you aware of other case studies?

[00:20:00]

John: L.A. County does a lot of business with private providers, service providers to the county: in the courts and in the probation department are two really big ones that strike me, and I'm sure there are plenty of examples in the health department, etcetera. That is not an unusual scenario.

Di: So maybe one of the interesting dynamics, then, here is that if you go back a couple of years, maybe there was a thought that identity provision, user authentication was a logical extension of some of the human resources capabilities. But that model of using the payroll or using the HR, that did not accommodate consultants and private partners, and so maybe that's a solution that an external IDP [identity provider] brings to the table that really wasn't possible a couple of years ago.

[00:21:05]

Would you guys like to comment about that?

Tony: If you look at your typical HR systems – your SAPs, PeopleSoft, etcetera – those have, in the case of Orange County, we have about 15,000 actual county employees. I have 26,000 entries in my database already or entities that we have as requestors. The difference is that we've got the business associates, the attorneys, the clinic workers, all of that out there – contractors – and everyone said, "Well, just use the HR." But again, HR databases are not always known to be accurate and up to date. We have, in our case, a situation where our HR, somebody might be on staff working for weeks. It's only when they decide that they need to get a paycheck that they'll get a record into HR.

If your timekeeping is only submitted every two weeks, then probably within two weeks you'll find out about it.

[00:22:00]

Meanwhile, they probably have given you access to data as an intern in a DA's office or some other, and you're working on cases. Again, we realize that there were differences in the time frames as well as the population, so that's why we split. But I think you're right in that, years ago, everyone viewed identity as it was only for the people in your closed system. But again, security without walls now, it's a variety of systems.

John: And HR does not have a lot of the information about what you are currently doing and what you are currently trained on and what your current assignments are. The people who are best positioned to know that information are the direct supervisors or managers, and so they're the ones that really need to maintain those attributes. The human resources department just doesn't even have that information. Those are important to making decisions about access to different systems.

[00:23:00]

We've heard the term the person who can count belly buttons is the person who ought to be the one who's vouching or doing the identity proofing around that particular employee and what their privileges are and what roles they're playing in the organization.

Tony: When we went to do policy, we'd meet with each agency and we'd say, "Okay, show us your documents. Show us what you do. How does it interface with the court? And then you send it to whom?" Just really walking through it in very deliberate steps. The issue is that a lot of times, John's supervisor might not have a very clear understanding of what he does, but his ***unit*** manager, being he's assigned to a unit – because these days, there's a lot of in-sourced, out-sourced, if you will, they'll lend somebody to a unit – so your unit manager would say, "Gee, we're all doing juvenile cases," etcetera in the case of a criminal, but that might not be his HR supervisor, so there was that difference.

[00:24:00]

Again, we really walked through the tracking of the paper documents to decide these policies and who gets access to what level of granularity. In our profile that we keep in the portal, we have functional title, we have what unit are you a member of, etcetera. A lot of times, it's the unit supervisor who's going to vouch for him, not his HR supervisor. You see the difference?

Di: Especially as people become increasingly interdisciplinary and matrixed and however else you want to say it: these informal professional affiliations that you have. Tony, I think you described one that was like, "Yes, your job title is probation officer, but today, I need to know if you are assigned to the juvenile division or the adult division or the reentry." Right, so could you speak to that? Or maybe you've got another case study of how that HR job

title is simply not granular enough and not timely enough to support –

[00:25:07]

Tony: I'll give you an example in the criminal context. You're an attorney. You're an attorney assigned to the public defender's office. It turns out that in Orange County, the public defender's office is actually three public defender's offices. We have the alternate defender, we have the public defender, and I've forgotten the third one –

John: The appointed counsel, alternate defense counsel, I think it's called.

Tony: So if you're a member of the alternate defense counsel – "alt" defender, that's right – the issue is you can't be accessing information from the others. So basically although your agency is public defender, your unit assignment separates the data that you have access to.

Di: Very purposefully for compliance with ethics rules.

Tony: Conflicts of interest, conflicts of knowledge, and it has to do with preparing for trial and who has access to what. In our case, the public defender might be suing the public defender, where one is an alt defender and one is the public defender.

[00:26:04]

So we really have to keep that separation of silo about your unit manager vouching that you have access to the case. And, of course, by going through the portal, better than, should I say walking the office politics? You have that authoritative source, auditable, that only you got to that data, no one else. I think that's a good example.

Di: I want to drill down a little bit, Tony, on this analytical process that you went through because I think it's going to be a best practice going forward. I think that for some of us, we have walked into a situation where we needed to develop privacy policy, and we asked the question, "Well, what would you like to see?" Maybe you could talk us through why that is the wrong question to ask.

[00:27:03]

Tony: My grimace is that in most of the project, what we did was we did everything on small scale. We did desktop exercises. We did role plays, and then we went out to the field. So the first thing is when you get these kinds of challenges out there in the audience, don't go out in the field. Do it among your trusted colleagues first several times in different iterations because once you're out in the field, rumors travel much faster than truth, and you may have shot yourself in a foot that is hard to recover.

In our case, we specifically found that by asking, "What is it you want?" we immediately were setting an expectation that was too high for Superman to hit. I highly recommend you not try that initially. Certainly if it works for you, fine, but we found that that was a bad tendency. What we wanted to do is, "What data do you have access to today? Can I see the document?" Again, going back to the very rigorous process of walking through the existing paper flow.

[00:28:03]

Through that conversation, we would hear from the clients that we met with what they would like along the way, and we would note that, but never, ever wanted to set the expectation, "Oh, I can get that to you faster," or, "Would it be good if that happened?" or, "What would you like to see?" Not that we didn't want to know that, but it sets the wrong tone.

We found that this was a very large cultural change anyway, this sharing of information in this form, using electronic and moving from paper to maybe a data screen, so we didn't want to stir the pot more than we needed to. Again, that's maybe one of those "hard knocks" lessons.

John: So you kind of start with reviewing the current process.

Tony: Definitely.

John: And then from the current process, "Well, what's wrong with the current process?"

Tony: Right.

John: "And what's right with the current process?" And then out of that, kind of take away from that –

[00:29:01]

Go away and figure out what kind of requirements for information they need, and then come back with kind of some straw man ideas.

Tony: Because if your informational interview at that first point, they left saying, "Somebody cares. Somebody's interested. I was glad I had the opportunity to express an opinion about what was wrong," that's a great exit for your informational interview at the first level.

You can come back to them later and talk about other things, but imagine contrasting that with: they leave, and they're thinking, "They're going to have it for me ready ***tomorrow,*** it'll be effortless, and I won't even have to log in." That's what they'd leave with, so you really want to contrast that. That's why I reacted a little strongly.

Di: I think that's really good guidance for others who are out there trying to go through the very, very difficult process of documenting detailed, enforceable privacy policies.

[00:29:57]

Tony: Again, the desktop interviews, the mockup interviews, having it real formal – everything we did with this project we had to do on a very granular level because it is cultural, it is business process change. It involves technologies where a lot of these people said, "Look, I like paper. I don't want to do anything different."

Di: The next question I'd like to ask you about your analytical process is that when you returned from these informational interviews, how did you gather together this huge volume of information about users and data resources and conditions and roles and all of these various attributes? How are you all managing that huge collection of attributes?

Tony: The small staff had to get this down to a table, so what we did was each of those resulted in a table with a very loose set of arrows that was the paper flow and then a set of check boxes that really is about your role and your suggestions, although the tables might have gotten long as you list their suggestions for improvements or what was wrong.

[00:31:02]

Tony: But again, you start to build a cluster diagram around what was the common sense that you got?

It is a lot of data, and it's all random, so trying to get some structure around it.

Di: There are some people who have approached this analytical process kind of from the top down, so an analysis of what the formal policies are, what state statutes say, what your county ordinances say, what your agency regulations say. But what I'm hearing you saying, Tony, is that that's really not the approach that you took. You took it from the grassroots up, is that right? Then did you check – the data that you collected in this table – did you check that against some of the formal authorities?

Tony: We went to the knowledge keepers, the tribal knowledge, and said, "They're doing this. Is there some regulation that allows that?" Often times, we found that there may or may not be a regulation, but that that is the culture.

[00:32:04]

Again, as the identity part of this solution, ours is not to reason why. On the court side, the challenge I have and we're working through over there – and again, we've got that strong executive advocate with the judge – working through how ***should*** it be there, as opposed to how it is today. I'm staying out of that change in workflow.

Di: You're aware of it, but you do not wish to be the decider.

Tony: It's a ticking bomb sitting there, and I want somebody to disarm it before I get near it.

John: You're just reflecting what the subject matter experts are presenting to you in a form, and then you ask them questions about decisions? "Well, is this permitted or is this not permitted?" And they answer the questions.

Tony: The paper record got to the social service worker as a formal request to the court. It then got to the child support person who the social services [case worker] was working with.

[00:33:02]

Now, I didn't see that as a direct request, and I don't understand how that child support officer got it from the social service officer without being an approved requestor from the court's perspective, but that might be the culture, and they might have been sharing that information on the phone or in some other method, so that's not ours to question. But maybe in the new system, there's a role for the child support person to log in and get the data directly. You see what I'm saying?

Again, that drives what we were talking about inside the identity providing solution as well as the service providing application. We need to have that policy with the granular levels. What data do you get to, based on your roles?

Di: Gentlemen, would you like to bring anything else out about funding, long term maintenance, project management?

[00:33:57]

Tony: I think the lesson I'd like to make sure everybody [hears] is: we've gone to a schedule that says we will do updates no sooner than quarterly. Because as soon as the user says, "I have a suggestion for you, and it's really good!" according to their friends, you have to be able to respond to that, either including it or not including it, but their expectation is that they hit the send button on that – we have a feedback button on our screen – they hit the send button, and their expectation is that tomorrow it'll be integrated. So we've set out a schedule that says it's quarterly updates, and we're going to allow the steering committee on the prioritization of the updates and their inclusion.

So those kinds of suggestions are – I don't know if you'd say they're standard in project management, but they're certainly standard in this kind of an identity development.

[00:34:49]

John: In terms of funding, I think that – in L.A. County anyway, with 44 different police agencies – establishing an identity provider for those smaller agencies where they can use the service to register their people and then, again, it's very similar to the model that's been described here earlier where they can be looked at as sort of external agencies, but they have to register in a standard way, and these are the attributes, and they've signed particular agreements.

That would go a long ways then towards giving them authorized access to a number of resources that you have in the county without them having to invest in standing up their own active directories and their own provisioning systems and that sort of thing. It might be one more ID for them, but that ID gets them to a wide range of resources.

[00:35:58]

I think in terms of funding or recognition that the county or the – well, I guess in your case, it's the county again – is a logical source for provisioning those other, smaller entities in terms of their identity.

Tony: In our county, we do another project, which is we do mass notification. We used a strategy that we came up with a while ago. We went to the vendor and we said, "We're going to buy mass notification for 3 million people, and basically we need this in the case of a disaster." So they said, "Well, how often do you expect them?" And of course, you come up with numbers. And we said, "But we'd also like to be able to let the cities use the same tool." Again, any time we could leverage these things, it was great. And so the smaller entities, smaller cities said, "I couldn't afford mass notification." But because we did it as part of a major plan, we were able to get in.

Incidentally, the second thing is that one of the scheduled applications for OCID is to take your profile information and push it into the mass notification.

[00:37:03]

Once again, you don't have to log into that database and update it again. We continually find ways in which having a single source is valuable, simplifying your life as a user and the effectiveness of your access. But how we get money out of that, I don't know.

John: One of the questions I get asked all the time – I'm just kind of curious as to how you answer the question – they say, "Well, if you have all of this identity management in one place, and they get access to all these resources. Gosh, if that ID gets compromised, now they get all these resources. Isn't it better that all these different resources all have their own credentials and IDs, because then if that credential gets compromised, it's only one system

they're getting access to and not 15." I'm just curious how you've addressed that, because you probably have heard that along the way somewhere.

Tony: There's the classic – it's called the "keys to the kingdom" argument. This is the key to the kingdom.

[00:38:01]

Tony: It turns out in identity, we don't do that anymore. Your key is the key to the identity. You don't know the rest of the credentials, so there's a hip and hop to get to those other credentials. Part Two is that we're using that intelligence I talked about before where we know more about you and have a higher reputation. It's not something you could write on a piece of paper. We data classify the systems that you get access to, so if you're getting access to a highly regulated piece of information, you might have to use a grid card. A grid card is a hard token, it's a piece of paper with four columns, four rows, let's say, and then –

John: It's something you have.

Tony: It's something you have in your hand, and when you get asked for your password, it's a PIN [personal identification] number you know, plus these combinations of the answers to the squares, to the Jeopardy squares.

John: You raise the authentication level.

Tony: And that raises your authentication, so now you're in two factor. Again, there are a lot of compensating controls when you move to an identity solution that didn't exist when you had random systems that you had log-ins to.

[00:39:02]

Di: Is that a good answer, John?

John: I like it. I like it a lot. Because it really is a convincing thing. All these application teams are going, "Wait a minute, I'm going to trust this identity management system? That's my job. That's what I do." And then they start throwing objections to why that's maybe not such a good idea.

Tony: We did an audit of many of their systems and found that people that no longer worked for the county, and they were still in their databases, etcetera. There's this value of having the full cycle that says, "I know that for one reason or another, where it's a question about his job role or his position in the organization. Has he been separated from the organization? Did he transfer to another agency?" By having the provisioning policy that says within the 24- or 72-hour rules, that'll be updated – that's vastly improved over the current process of having somebody's credentials who hasn't been there for a year. And he probably wrote it on a piece of paper, and it probably didn't get changed in a year.

Now, we change the passwords on a regular basis.

[00:40:04]