Enterprise Transformation in Challenging Times

SUMMARY KEYWORDS

agencies, modernization, cybersecurity, enterprise architecture, cios, people, understand, federal, programs, fisma, issue, business processes, architecture, talks, cio,federal tech talk, technology, service, systems, omb

00:14

Our guest today is Mark Forman, former First Federal Chief Information Officer, currently executive vice president at Dynamic integrated services. You know, Mark, I've done over 900 interviews, and I carefully watch my downloads. Whenever you're on my show you move the needle, I think this is because your depth of experience gives you deep knowledge of digital transformation in the federal government. You've seen successes and failures. Here we are in March of 2022. And the federal government is challenged to respond to a what some people call New World Order. So Mark, are we at this tipping point where federal leaders will get serious about digital transformation?

00:52

Thanks, John, for that nice introduction. I sure hope so. I think that there are some things that are the same and some things that have changed. I don't think there's any question that over the last couple months, the understanding of cybersecurity is much more widely spread across the American public than it was even a year ago. And I hope that that's the case for the executive leaders, the political appointees in these agencies, that they to understand the implications of cybersecurity, on their operations. I suspect that's the case. But I think there's also a chronic problem that occurs in every major technology shifts, certainly the.com era or what we call the government, the notion that you had 35 or 3600 government programs, and each program treated its customer as if it was unique. And all the studies show the citizens looked at government, they didn't differentiate and you program, the more forms they had to fill out, the more complex they saw the federal government, and sometimes they just don't fill out those forms. They don't go for the services that they need. And that's the question for me is whether the agencies in the White House understand that there aren't 3500 different customers, there's one customer for the government, and they need to provide that integrated solution to enable people to come to government.

02:19

You know, I seen a lot of things going on the federal government here. And I look at the federal leaders who are appointed, then I see the technology people have kind of risen through the ranks. And there may be a disparity or or I have a friend who works in hot with medical, he talks about gap analysis. And is there a gap analysis between, you know, some of these federally understand the threat from cyberattacks and, and maybe the political appointments just don't Is there a gap there?

02:48

There clearly has been over time, like I say, I hope it's declining. But cybersecurity is really at its heart about information security and being able to maintain the operating processes and practices of an agency. It's using the term cybersecurity or IT security or Federal Information Security, modernization, FISMA, the fist cam, which is the core layer for smashes that all sounds so geeky that I think a lot of agency political appointees assume that's the role of the the it geek, generally the CIO or the CTO for an agency. And they forget the linkage between their dependency on information processing and IT security and the operations of their agency until they have a major cyber incident.

03:43

I've spent a lot of time in the commercial world. And if you have a large project, and you're trying to convince a company to go with this little initiative, you can have everyone in the whole company convinced but if leadership on top doesn't have buy in, if they don't believe that cybersecurity is important, or they don't think that changing project management is important. It ain't gonna happen. It just it's gonna it's gonna die on the vine. And I think this whole buy in from leadership, especially the higher leadership is important, isn't it?

04:12

Well, certainly is. And I would add into that, that most agencies are overrun with complexity of their systems. You raise the point are we really going to see this shift to digitization? And I think one of the the issues is for most agencies, certainly the Cabinet departments and agencies, they've done modernization by adding on to their legacy systems. So they've created this spaghetti of customized interfaces. And let's take for example, zero trust. Zero trust operates where you allow access to the systems. That means it's got to go through the middleware, the messaging systems, and there's so much that's customized in the spaghetti, it becomes very expensive, time consuming, resource consuming main energy consuming for the agencies to put in place zero trust. And yet that operates at that area of the business processes where the risk exists on the business side. I don't think the political appointees understand that. I don't know if they have the energy to dig in and understand that it's not it's not simple. It's not like reading a Marvel comic book. This, you know, it's it's, it, it is a complexity issue. And as these jerry rigged modernization attempts have occurred, and the spaghetti of systems system interfaces, it's just spread complexity in the agencies. And I'm not sure I mean, I think this is the critical challenge. Is there a way for the IT industry to simplify that complexity, and simplify the transition out of that complex environment into low code, no code environment of the cloud?

06:04

Let's jump over the heads of the political appointees. Let's go up to Capitol Hill. And take a look what's going I mean, if someone wrote the history of 2022, they'd look and say, Well, geez, you know, there's been a lot of reaction to this. And, and prior to the State of the Union, the Senate passed a strengthening of American Cybersecurity Act. It mentioned that you just mentioned FISMA talks about FISMA talks about FedRAMP and secure cloud improvement. What are your thoughts on this thing? This is addressing some of the issues or is this just another checklist act that may not be actually deployed? I mean, that sounds sweet to the house right now. It looks like it's got bipartisan approval.

06:38

Right. I think that these initiatives are a step forward, because they're refocuses the energy of leadership on it in agencies. Now, the question like was the issue with FEMA, sorry, with FISMA, we always start out. And certainly we had this FISMA passed while I was at OMB, where you get the heads of agencies to consider this, it's really important for the President in the Cabinet meeting, to make his or her understanding of what needs to be done. hit home with this cabinet secretary. Certainly when I was at OMB, we had that with the President's management agenda. And every quarter when the progress in the status reports were given to the cabinet, if somebody fell down, and the issue was it, security is why their score fell down, or their progress fell back. The cabinet secretary had to explain to their colleagues in the cabinet and the president, what was going on what they were going to do to fix it, that kind of governance, insight, and oversight drives action in the agency. If it's not an issue for the cabinet, it's probably not an issue for the Secretary until there's a crisis. And by then, of course, it's too late.

07:58

I want to ask you a question about enterprise architecture. But first, I mean, I'm in the classroom all the time. And and one of the best ways to keep up with the fast changing world of technology is to attend webinars, you learn that your schedule, and you get continuing education credits, I think the best webinars are from Fed insider.com. Just last week, they had Steve Fernandez on from the Department of Education, talking about zero trust

back to Enterprise Architecture. Boy, that's a big fancy word. When I first had someone in the studio 10 years ago, they walked in with this laminate 11 by 14 sheet with eight point type. And and they handed me like, it was like a big prize, like a cat would bring in a mouse or something. And I said, How do I need a microscope to understand all this enterprise architecture stuff? In a previous interview? You did? I thought you hit the nail on the head, you talked about well, you know, what leaders should do is they should look at their see their architecture now. And look at their target, maybe their targets, say architecture, it should be in the future. So that really is is a high level view of what the best transition is for digital transformation, isn't it?

09:01

Right? When we originally coined the focus on architecture in the clear Kodak, it was really on the information architecture. And the first versions, many people may remember the federal Enterprise Architecture Framework, what people used to call the FY F was an information architecture. When I came into OMB, we shifted that a little bit to focus on what we call the federal Enterprise Architecture reference models. That was a little bit more of how do you take advantage of technology to drive improvements in the architecture. Every agency has an enterprise architecture, they may not have it documented, but that basically describes their information management environment. And ideally, the business processes serve a purpose in terms of the performance of that agency. those business processes work off of data, and the tools that pull To gather the data with the workflows, our technology, tools, applications, and of course, applications run on infrastructure. So much has changed. And I think it's so hard for agencies to take advantage of what's changed in that underlying infrastructure and the applications, Cape capabilities to run those business processes. Unless the agency starts to look at where are the opportunities in these cloud computing platforms. Unfortunately, what's happened is, I think too many agencies have done point solutions. So you see a department that will have ServiceNow, Microsoft Dynamics, Salesforce, maybe three or four other homegrown case management

THE OAKMONT GROUP

systems, and they're all competing for which is best, and no real way to architect, which is best. And if you have multiple case management systems, that generally breeds confusion for whoever the public is, it's being served by that agency. Oftentimes, there's inconsistency in the data. So a decision made on one system screws up, what's the service being provided in another, oftentimes, because of conflicting data, and these customized interfaces, you can't tell if somebody has done identity theft and identity theft, I think is a growing issue, confronting the agencies, as well as in the commercial world.

So to be modern, and to figure out what to fix in your existing architecture, you have to understand where are the opportunities, you can't do everything at once is not affordable, choices have to be made. And that's this concept of using an enterprise architecture to develop your target view of your IT environment, understand the trade offs in terms of cost and performance and act accordingly.

11:56

I'm recording this from my office in my house here, and I look around the house and I got less stuff to do. We got painting, landscaping, you can't tell once you got to set priorities. And federal IT leaders have to set priorities as well. You've been in that seat, you've had that, you know, you have the t shirt, thank you on the t shirt, and the hat and everything. So So what are the priorities today in March of 2022? What What's What if you could get a whole bunch of CEOs around one time and said okay, you know, listen up and write this down? What suggestions for prioritization? Would you give them?

12:28

I would, I would suggest how they do it, not what they do. Ah, because I think that the key is how the SIA, CIO and CFO work together with their program offices. There's been so much focus in hearings bringing CIOs up to the Hill to hold them accountable for resource decisions that they simply don't control. They have oversight. They can act as a naysayer. But the reality is even in the US Code, still, the programs are responsible for defining the information resources that they require. The CIOs and CTOs under both the it reforms like Claire Khan and FITARA. And the evidence had CIOs and CTOs is supposed to recommend and identify ways to optimize the use of the technologies and data to improve the business processes of the agency. But I think most CIOs and I think this is what comes out in the hearings. Most CIOs and CTOs don't really have the ear of the program offices for a variety of reasons. You mentioned Congress before, Congress funds programs. If you look at the budget for the CIO, or what's called the salaries and expenses of the agency, it's generally a fraction of what they fund in the programs. And so each program has an incentive to deliver its results. What the CIOs and CFOs have to figure out is, how do you work together with those programs to identify the opportunities for leverage shared services and performance improvements? So it's the process that I would recommend.

14:12

Now, when you said the word for Tara, I thought grades scores, and I give out grades my wife gives out grades. And what we can say in general since COVID, grades have probably been inflated. That's in high schools. And so what about fatigue? You think COVID caused great inflation with the star scores?

14:31

You know, I think it's really hard to tell. I think those are very subjective. They try to tie to objective data. I actually look at those to see who's not graded highly, or who has consistently low grades to understand where there may be issues. And inevitably, what I find is that the agency leadership doesn't view the CIO as the source of authoritative insights.

15:04

My mind, that's a good observation. We did an interview about eight months ago, we talked about agile software development. And I'm sure you can give us an eight hour lecture on Agile software development big projects. So in our current environment, increased threats. What role does Agile Software don't play?

15:22

I think that if I were recommending a CIO, what were the two most important things to focus on, one of those would be bringing into their agency, a modern software factory concept. The Software Factory concept has been used in the commercial world and other governments around the world for several years. And the notion is that you have to have high quality agile development processes, to do your applications maintenance and modernization for your existing applications. I think agile and DevOps are at the core, these these practices that speed and make user friendly, have simple things like bug fixes, or new features and functions, and of course, regulatory changes that need to be implemented. So I think that's very important. The other thing I'd say is, modernize and improve the body of your portfolio management and your capital planning investment control process and utilize portfolio management. In that context, you know, for new systems, or for existing systems every three years, the agency should be looking at how do we take advantage of the technology to better improve the performance of a mission. And that could involve creating a new application, it could be involved modernizing existing application, but you can't do anything in modernizing your building new if you don't have that high quality software, factory model operational.

16:55

Yeah, I love when Elon came up with the Kessel Run up in Boston, just place it right next to the MIT and bring in the smart folks. You know, what a great idea, you know, Software Factory up in Boston. I am doing a podcast and I listen to podcasts. I listen to a wide range of podcasts, cybersecurity podcasts. And so I listened to one where a gentleman uses kind of rough language. And, and he said, You're not You're an idiot, if you don't use multi factor, administration, or authorization MFA. I said, Well, I don't know if I'd be strong enough to say that. But I would say something like you can phrase it in a way that yes, you would highly recommend multi factor authentication, wouldn't you?

17:35

Yeah, absolutely. I mean, at this at this stage of fraud and cybersecurity risk, I think that goes hand in hand with zero trust. I think there are other elements of that in the zero trust model, such as are you using tools that you normally use? Is the device registered? And is it clear that you're using one of your known devices to do something that it's known that you typically do? I think the multifactor authentication and the zero trust approach go hand in hand. And I think it's got to replace role based authentication approaches.

THE OAKMONT GROUP

18:20

Yes, cognizant, he would call that our backward and they are BSC or something like that. Yeah. I am looking around I was in downtown DC the other day things are slowly starting to open up I'm in the classroom now face to face without mask. It's, it's everything's changing here. So there may be events, believe it or not face to face events that are coming up on the horizon. So if if you're listening to this and wondering where you could learn more, you're kind of interested. We've been to tons of events where what what do you think, a couple events that my listeners should attend, just to get a better idea of this whole idea of enterprise transformation in challenging times?

18:55

Well, to be quite honest, I think the hearings now that so many of those who've done live online, especially if it reflects your agency, you know, whether it's the House Government Oversight or Senate, Homeland Security and Governmental Affairs, I think there continues to be interest, you know, certainly the photogra hearings. But then I think there are other subcommittees now that are looking at it modernization that IT spending, and some of the issues that I see are not unique to those agencies. They're replicated, but to understand how Congress is looking at this, and what Congress might be do doing in response, I think is very important for people in the community. One particular subcommittee I like is the VA modernization house Veterans Affairs IT modernization subcommittee, I think they have terrific oversight hearings, and the members understand so many pieces of the process, not only the systems being managed well as a project, but also the role of acquisition and how to move forward on both a plan for modernization and an acquisition approach. I found it tremendously informative. And I think they share their information with their other colleagues in Congress. So I think that's that's one error. And then of course, I think that there are a variety of organizations, I like a tox presentations, like affirms, presentations in in, I think there's some good ones in akaya, as well. And of course, your podcast. Yeah, for licensing. Insider. Yeah. Yeah.

20:52

Because, because the bad jokes, you know,

20:56

find sites.

20:57

Yeah, I was asked by my guests. Show me the money. How could this save me money? But that questions been asked to you I was at an event or webinar or something with someone turned to you and said, Oh, yeah, Mark, all these highfalutin ideas, yet they show me the money. And you said, well, the technology modernization fund, and then it kind of shut him up. Yeah. And so so give me your crystal ball here, the TMF detector? Is that really gonna catch on? You think that's a really good idea? I think this is a good solution to our current crisis?

21:25

Well, look, I think the I think there are changes that are needed. First of all, I think the funds been diverted to supplement cybersecurity spending in agencies, not only because they don't have enough money in the agencies to do cybersecurity, but they don't have an agile enough budget process. And so I think the technology modernization fund, has rapidly become the agency IT security addendum fund, or supplementation fund, if you will, there still needs to be a focus on modernization. From my perspective, and I think there's been movement in that direction before the executive order in cybersecurity, investing in shared services, and creating a shared service in this cloud platform environment that we're living in which then agencies can adapt. It's very useful, you know, Enrollment Services, which dominate these, these 35 or 3600. Programs are essentially Business Rules Engines, you fill out a form, and the forum hits up against business rules. And most of the people are approved. They're always the outlier cases, they have to go through appeal process or need somebody who's essentially case manager to adjudicate, but, but for a lot of these forms to go through a common enrollment process could achieve what the President had in the customer experience executive order. I thought it was a very interesting model, reduce the time tax

23:12

and duplicate information. I mean, it just opens up all kinds of worlds of trouble, doesn't it?

23:18

Yes, sure. So. So that's, that's a model where you literally could have cost avoidance or creative payback by agencies taking advantage of a shared service and funding that shared service, it would fit the Economy Act, and the TMF concept very well. And I think it's incumbent on OMB to work with the CIO console, and the President's Management Console. I'd add in the chief data of Sue's counsel to look for opportunities where you can leverage technology to share it service, because there are data management and our business process workflows that are essentially common. Get off of these legacy, custom build systems, and understand that these things have been built hundreds, if not 1000s of times, and there's not that much unique, the business rules are unique. That's a configuration issue. The workflow is what cloud services support nowadays.

24:18

That's great. I really appreciate your time today, Mark, you have been listening to the federal tech podcast with John Gilroy. I'd like to thank my guest, Mark foreman, former First Federal Chief Information Officer and currently executive vice president at Dynamic integrated services. Thanks, Mark.

THE OAKMONT GROUP