67. McGann, Parente, and Zahadat:

Cybersecurity in Project Management

Susan Parente: As project management professionals, we are being asked to do more. First we were asked to understand our customers better, to understand business value better. Now we're being asked to take responsibility for IT security.

Nima Zahadat: Training is becoming more and more commonplace, but the issue is, these trainings are extremely fast, extremely compressed. Instead of doing a training which is ongoing, where people attend on a regular basis, they've taken the approach of, Well we'll just send them to a three-day training or a five-day training session, and then that should do it, and if they get one of these certifications to go along with it, then all the better, not realizing that that really doesn't protect them.

Chuck McGann: We work really hard to make sure that security is not a burden. It has to be in the background. It has to be just intuitive to everybody and it has to just function. It has to enable the business, it can't impact the business negative.

Kendall Lott: The threat of a cyber-attack and it's probably the biggest risk that every business, every enterprise on this planet faces. We must constantly be on guard, and vigilant. We're releasing this very important episode of PM Point of View® in October, National Cybersecurity Awareness month, here in the United States, a collaborative effort between government and industry to raise awareness about the importance of cyber security, and to ensure that we all have the resources we need to be safer and more secure online. Project managers, you're at the forefront, engaging with teams, working virtually, sending and receiving artifacts and communications. Cybersecurity should be among the first things you consider when setting up and kicking off a project. More than just establishing systems and safeguards, cyber-awareness needs to be embedded in the culture of every project.

With the help of Alison Gonzales from our sponsor, Essential Assets Group, I have gathered a round table of experts: Chuck McGann, Susan Parente, and Nima Zahadat, to go over behaviors and best practices to keep your project as secure as possible. You don't want to be the gateway of a breach.

Announcer: From the Washington DC chapter of the Project Management Institute, this is PM Point of View®, the podcast that looks at project management from all the angles. Here is your host, Kendall Lott.

KL(02:24): We are here today to talk about cybersecurity on the PM Point of View®, and how that works with businesses and ultimately how it's going to work with project managers, what we need to be thinking about as we all enter the no longer new, but certainly still the brave world, of cybersecurity and this podcast is sponsored by Essential Assets Group.

Allison Gonzales here helping us out today, and thank you for orchestrating this and organizing it.

So what we'll start with is introductions. So we'll start with you, Chuck.

Chuck McGann (2:52): My name is Chuck McGann, and currently I am an independent Cyberecurity Consultant. I do cybersecurity education, mostly to executives today…a lot of practitioners running the gamut from certified CISO to asset management. And I'm the former CISO for the US Postal Service. And as you probably are aware, the postal service is one of the largest organizations in the US, with a number of connectivities, it's a Class A network. So I learned an awful lot about cybersecurity and protecting customers' data. When you figure out that every person, certainly that gets mail, is a customer of US Postal Service. When you're trying to protect that level of information, it really does make a difference on how you plan, how you perform, how you react and how you schedule and how you work with other people.

KL: Thank you. The only thing I'd throw in is CISO. That's a great title. Everyone needs to know what that is. That's the Chief Information Security Officer.

CM: Yes, that's correct.

KL: Excellent. So our PMs, may be familiar with those people inside their own organization. So it sounds like we're talking not so much about security projects, but rather the element of security that's embedded in a company, and that's what we'll talk about in the role that project managers might have bumping up against that. Which takes us to our project management guru in the world of risk, Susan Parente.

Susan Parente (4:15): My background is actually in mechanical engineering. But I got into software development and then project management with that, and I'm now a Project Management Specialist. Project/program portfolio, and my subject matter expertise is in risk management within that arena. And so my focus is on cybersecurity awareness, realizing that it's an important aspect of every project, in managing every project.

KL: So trying to move into awareness and beyond being reactive. And seeing how that works from a PM's point of view. Then there's that whole scenario where there's taking the complex and making it complex and that's where we bring in Nima.

Nima Zahadat (4:57): So my name is Nima Zahadat. I'm actually a professor at George Washington University, and I also do some work occasionally as a contractor for various places, primarily dealing with DoD and most of it deals with training in various aspects. It could be security, it could be be management, it could be big data, it could be programming.

KL (5:25): So tell us a little bit about the framework that you're familiar with, coming from a more structured and academic background and particularly around the NIST requirements. What is this kind of…real rules of how we need to be looking at cyber within organizations, and security, broadly?

NZ: Well, NIST has a frame work. It's called the 800-37, and it's in Release One, as I remember correctly. They have not moved up from Release One yet. And they call that the Risk Management Framework, And the idea is that it has six stages that you need to go through to identify all the risks and address all those risks properly. Now, once you have the framework in place, and this is

something that does take some time to obviously implement correctly, then you can fill in the little, shall we say placeholders, the templates that you've taken and put in place with areas of your organization that need to have particular controls put in place to handle the level of risk that you want. That's more or less how it works. It is not the most fun publications to read, it's kind of boring, and it usually takes two or three iterations of reading, going through them, to have them make a lot of sense.

KL: Okay, but let's bring this down to a level where people can get a sense of this. Two questions: Why did they decide that they needed to set up a framework for people to use? And what are those publications addressing? In lay person's terms, what is it we're having to look at?

So it's the…Why do we need it? Why did they make a standard? And what is it that we're actually framing that people like a CISO have to respond to, and a project manager has to be aware of?

NZ: The reason they framed them was because Congress asked that it was created. So we had the various congressional acts that were passed, in particular FISMA. But that required that all the executive branch agencies must have certain level of risk management. And NIST was tasked for coming up with the necessary…I don't want to call them standards because they really aren't standards, they're more like guidelines. They were tasked for coming up with these various guidelines, and the 800 series was born. They did not need to do that. They could have gone with an ISO standard or the Department of Defense standards, but they decided to basically come up with a new guideline, set of guidelines, I'm saying standards myself, that they came to be known as the 800 series, and it's been…each publication has gone through some revisions since its inception in the early 2000s.

KL: So, what does it tell us to do? What are the high level things that it's addressing?

NZ: The high level things that 800-37 asks is to first identify the risks, then go through and select the various controls that are necessary for implementation to protect the organization against these risks.

When you identify the risks, you also have to pick a level of, shall we say risk management, meaning that you cannot eliminate the risk. So there'd be no controls that can eliminate risk, the best you can do, you can say, Well this is a level of risk I'm going to accept. And these other controls I'm going to put in place, whether they're technical controls, administrative controls, to try to protect the organization. Once those controls have been recommended, they need to go to an approval process, and once they are approved, then they are implemented. Once they're implemented, then they are routinely assessed and audited. And that's the 800-37, for instance, that goes through the process of, How do you go about assessing and auditing these controls that are in place? And this is a circular life cycle, that you, as you assess and you find that there may be issues, there may be areas of improvement, you make those changes, you go through the process of getting them approved, you implement them and the assessment continues.

Of course, as technology changes, as processes change, as business model and business goals change, then these assessments catch up with that, and they may have to retire some controls. They may have to bring in some new controls, there may be new risks that will be identified and some of the old ones that need to be basically dispelled, saying we don't have that risk anymore, so we just get bit of those controls and those equipment and those positions, shall we say.

That's basically the process. That's how it's supposed to be done. Like anything else, initially, it's difficult. Once you get... Once you implement it, and you go through it a few times, then it becomes pretty much just straight forward, and can be done fairly quickly and easily.

KL: So there's a broad level of risk management, risk identification going on, here as well as there is some focus it looks like on the information side with the FISMA, with the Federal Information Security Management Act.

So, Chuck, we're talking about the identification and management of things with proper controls. What did you experience as a challenge in trying to address that, and how does that affect people in the management layer?

CM (11:13): So one of the bigger challenges obviously is that all these…implementing all these controls takes budget, it takes money. And the challenge there is when you run across a business owner and the business always has the opportunity to say No, within the FISMA controls, within all these controls. The business always has the opportunity to sit there and say, “No, we're not going to do this, we are going to accept the risk,” as Nima said. “We will determine what level of risk.” But when they sit there, and try and balance how much money does this cost me, and I use this kind of analogy I’ll use now when I teach this class: I have a $100.00 horse. How much fence do I put around a $100.00 horse?

So if I have a... If I have an environment that’s worth minimal, if you would, how much money do I spend? And as an executive, you have to sit there, certainly as a CISO, you have to sit there and, number one, make the assessment of what the impact is to the business should you lose that particular application or should you lose that particular ability to use that data or should…You know, What's the exposure?

And then when you identify the exposure and the risk, then you sit there and say, “Okay maybe it's small, medium, large, or moderate,” and then you have to come up with a strategy that says, "By the way, executive team, I need a million dollars to protect this $500,000.00 environment.” And what you're going to experience is probability. Management's going to sit there and say, “What's the real probability?” And that goes kind of back into the heart of, again, what Nima was saying, you do the whole risk assessment. And that's part of, in my mind, when you're actually rolling out a project you have to keep that in mind and security, up until most recently, has not been part of project planning. And that budget requirement has not really been part of project planning. And we're getting it more and more and more at the project planning. But a business owner in the past has always said, “No, no, no, security's not my problem. Paying for security is part of the whole…that’s what you guys do. And now with budgets being as constrained as they are, security departments don't have the ability to say, I'm just... I'm going to put all these controls around you. Because you brought this application in, you need to pay for this. It needs to be integrated into our overall environment, it has X amount of dollar value to the company. And as an executive, you...there's a CISO executive, you have to sell that. You have to convince your company that it matters to them that this risk, this exposure, could have a detrimental impact to them, whether it be financial, whether it be reputationa, whether it be operational. So you have to kind of go through that environment to say, “It's worth us to spend X to protect Y.” And what you're going to have obviously is, people, executive business owners, will sit there and say, "Well what's the worst they can happen?” Well the worst that can happen is you could become an open door to any of your business partners. You

could become an open door, and people can mine all your data and just continue to add all that data to something else.

So it's not a simple, you know, “We have to do this control.” Because you don't have to do a control, it's a guideline. You can sit there and say, “No, we're not going to do it.” And there’s four things you can do: you can accept the risk, you can mitigate the risk, you can transfer the risk, by trying to get somebody else to do the work or buy insurance for it. Or you can just kind of say, “Nah, we're not going to do this work anymore.” You can Not do the work anymore. I had one company that said, "You know what, it's too costly for us to implement these controls, we're not going to carry that business line forward.”

KL: It's more than having the team, then, that can do the analysis. As an executive, you're doing the moral suasion. You’re making a business case, and I'm hearing hints and allegations underneath this of, it's really a change management problem. Because people have to believe it matters. How do you feel about that?

CM (15:05): So it is kind of a change management problem, that's where a CISO has to understand socialization. When I say socialization – socialization of controls. If you walk into a meeting and say, “I need to put these controls around there.” And you haven't socialized that with the people who actually do the work every day. You have put yourself at an extreme disadvantage.

If you haven't worked with the business owners’, how shall I say, movers and shakers, the people who are going to have to implement some of these controls that you're trying to ask them to do, you will not have an easy time. Because, number one, you're asking for money. Number two, you're putting impact probably on their product or on their application.

We work really hard to make sure that security is not a burden. It has to be in the background. It has to be just intuitive to everybody, and it has to just function. It has to enable the business, it can't impact the business negatively. Because if you impact a business negatively, your security is going out the window. It’s just not going to happen.

KL: I'm thinking that part of that has to do with how you make a compelling message down to the people who have to do work and are engaged with that. How did you address the awareness function from where you were sitting, making people aware of the controls and the need for using them?

CM: That's a really interesting question because we kind of went through two different iterations of it. Years ago you started with, "Here's the canned security awareness.” You know, everybody does their one hour a year, and you try and give them blurbs every once in a while. And then we kind of worked our way in the role-based security. One of the companies I'm working with now, they kind of... Everybody doesn't need to know all about security. They need to know, number one, to identify when something is not right. And then they need to know what to do when something is not right.

So that's one of the things is that we tried really hard to say, if you see this, it's kind of like “You see something, say something.” It's kind of like that. If you see something that doesn't look right, let's say when you left on Friday, your password was X, when you came in on Monday your password didn't work and you tried it a couple of different times. You really need to talk to somebody in either IT or in security and say, "Let me take a look because that might not be right.” Or if you sit there

and say if you're already… if you get a message that says you're already logged on. And those are some of the security controls that we talk about in 800-53. How many log-ons can you have? How many log-ons can you be allowed? And if you find yourself that you're already logged on, well then how am I logged on when I'm just trying to log on today? Somebody got my credentials. Those are some of the things that you look at in the security awareness thing. So you try and educate to the level of where people would be able to identify a threat to their particular world. And then obviously your security people are continuing to be educated on what to look for in log files, log file analysis, volume, traffic volume, things like that.

KL (17:57): Susan coming at it from risk management, from a project level, right? So the project manager should be aware, and should be receiving these messages from their organization, perhaps from a CISO. What is the key set of things or topics that a PM needs to be aware of in the security space as they're looking at risk?

Susan Parente: Well, first of all, to kind of catch on to what Chuck just said, there's actually a Verizon 2015 Data Breach Investigation Report that said 90% of successful cybersecurity attacks succeeded because of human error. So...And Chuck is nodding his head, which you can't see on audio, but this relates to that. And I think it's great what Chuck said about training needs to be applicable to that person's role. Not everybody needs to be a cybersecurity expert, but people need to be aware of how they become a risk or a target or how what they do can add to things.

One of the big things now is phishing attempts. So you get a link in an email, and they look so amazing. Now. I actually got a PNC Bank notice. Well, I don't have a PNC bank account, but it said you need to click on this link and do whatever before something goes wrong. It creates this whole like hyper situation. And I knew it was a phishing attempt, and it was a great example. They're becoming so good at doing that. So it's about how do you educate people to know, Don't click on the link!

Even if Kendall sends me something, I don't click on the link, unless I hover over the link, it looks legit, Kendall told me he was going to send me something. There's a lot of things that have to happen and I even got tricked once, because somebody said I'm going to send you something, and the next day, and I got something from them, and it was a phishing attempt. And that was just a bad timing incident, but if they had sent me something, and they didn't say they were going to send me something, then I would have called them. So you know, it's just constantly being one step ahead with that.

KL: From a PM's perspective, what is it you're trying to get them to highlight?

SP: Well, I think the big thing for PMs is what I see with risk management and IT security. It either happens at the end of the game. So this is the one failing, is you wait until the end of the project to get IT security involved, and then it's like, "Oh wait a second. All those things we did. We have this architecture to the system that is actually flawed. That it creates risks for security that we didn't realize." Okay, so that's a bad time to get IT security involved.

The other bad thing I see happening in project management is we list a whole bunch of risks, we do all this risk identification, which is really wonderful. Check the box. We did risk management, and then we just go off and execute the whole project, and ignore risk management during the project. So neither one of those is a good solution.

SP (21:03): What a good solution is, is to be risk aware, risk mindful throughout the project on a regular basis. Not leaving it up to the IT security people. The IT security people…there are not enough of them for all the attacks there are. There's not enough for them to see everything going on, like Chuck was saying. So the project manager needs to include that security awareness as part of the actual requirements for the project. So they need to listen to the customer, what the customer wants, and consider that security is part of what adds value to the customer. And this is going back to what Chuck said about what is the actual cost? So yes, we identify all these risks, but we need to assess them. And in that assessment, we prioritize them. And then we decide based on that priority, how we're going to actually manage them.

So the controls that we put in place are going to be dependent upon that assessment. If something is not likely to happen…very, very unlikely to happen probability-wise, but the impact is huge (so this is like the meteor hits the building, the catastrophic God Act, etcetera) we have to have a plan for that. But we may not do something to reduce the probability of it occurring, because the probability so low. But we do want to have a plan if it happens.

SP (22:27): So that ends up looking like continuity of operations. And for project managers, yes, we have this project, it's finite, we deliver this product, service, or result and then we're done, but we also need to be responsible about what happens, they put that product into production. If it fails, what's our backup plan for that product? And that's going to depend on what the value that product has.

So is this for DoD or is this for Department of Education, and what kind of data is it, and what kind of information is in there? And basically what's the cost impact to the organization for a failure for whatever that looks like, either the systems doesn't work or data gets taken from the system. What those risks are, are going to be different for every system, and so that has to be evaluated. And then what's the cost? And then decide what you're going to do.

KL (23:29): Project managers have two levels we're looking at. It's almost like at the kick-off meeting would be a great place to talk about what this organization requires from a CISO-standpoint. How we will store information, send information. It's almost part of communications planning, it strikes me. The other one was what you're talking about, your actual product. Broadly looking at risk management around the product and your ability to produce the product. I would imagine in some cases, there's some controls there that we need to think about if there are information technology products anyway. But from our team's perspective, do you discuss their ability to handle it early in their own planning as a way of behavioral…how they're going to behave on this project, how they're going to act on this project?

SP: Well, from a project management perspective, I've always involved the IT security team early on, and that's not the case of a lot of my peers. So they tend to involve them later in the project, and I think later is too late. I think when you're looking at what are the requirements for the project and you're doing planning, that's when you involve them. And if it's an Agile project, same thing. It doesn't matter if you have a product backlog or you have a list of requirements, there's still a security aspect to consider and the customer needs to be involved with that. And the thing about IT security professionals, they're going to look at it from that perspective. The customer may not be able to see that perspective, but if you have them in the room, they can share what that looks like, then the customer can decide, "Okay what that person said, Yes, we care about that." Right? But the

customer needs to hear that; they need that subject matter expert to share with them. Here are the concerns, here are the bad things that could happen. Because they don't always realize those because they may not have that view, that perspective that IT security people have, they're kind of always looking from the perspective of, What could go wrong? What could break this? How could we lose data? The customer doesn't think of it that way. A lot of times the customer's "Oh, stuff like that doesn't happen. That only happens on TV." Or, "It only happens to a large company. It only happens if you're Department of Defense." And it's so not true anymore. The threats are not just global threats. They could be competitor threats. There's a lot of books and writing about that now, where companies are going after each other and trying to get data from each other for competitive advantage.

Everybody has competition, so we need to be more aware of what the competition looks like now. Unfortunately, it's not as friendly of a competitive environment as it was 20-30 years ago, and I would not trust my competitors with my data by any means.

KL (26:21): Well, that opens a whole new world about what we're doing with who we are trusting with our data as we start talking about cloud and the fact that everyone's using social apps, to be able to communicate and share, as we look at some of the... I'm thinking some of the software we use to do project management has some potential breaches in there. It's really common now to use a lot of different software that gives us kind of Kanban boards, where people are sharing data about what they're developing and how. Slack is really, really common, and other messaging systems as well. What are you seeing from a security perspective on that?

CM: Yeah, so I think part of the challenge, in fact I use Slack in one of the committees that I'm …actually two of the committees… I'm on. But it's protected on a joint kind of environment. But we don't put anything out there. We may use a secure Dropbox kind of environment to share a file or to share something that we want to keep relatively close to the vest. But within the social channels, if you would, I think people share too much.

KL: Let's take it to the project managers. They are going to be using different software to communicate with each other and... And that's always been true, so I don't want to go over that in the same sense. Here's what I'm thinking is this: We are highlighting to project managers that they must collaborate more. It's the soft skills. We need to do better collaboration instead of sitting in the office and saying, "Show me your gantt chart, and I'll tell you if you're behind."

We're talking about using these things because we are trying to generate more creative thought, more rapid turn-around of information so that people can continue to stay on focus, on task. It seems to me that, though that that possibly raises challenges, or does it?

CM (27:57): You have to make sure that when you're in the project management environment is the need to know. Not everybody needs to be aware of every project and all the details, the gut details if you will, of a project. High level…I don't have a problem sharing high-level project information. But I don't know that everybody needs to know unless they're a particular level, you know, a coder doesn't need to know who's making decisions necessarily on budget. And they don't necessarily need to know what all the budget numbers are. But by the same token, a peer manager might be interested to know how much he's expected on his side to contribute to an environment or on a project that's shared. So within environments, I think as long as you've protected the fence around your own organization, within your own environment, I'm a firm believer in everybody has a stake

in success. So if it's my project, your project, Sally's project, Bob's project, Susie's project, everybody has a stake in success.

Now there's competition within projects and you're going to be competing for resources, you're going to be competing for the particular people and money and things like that, but in order for the good of the company, you have to be able to sit there and say, "For the good the company, I'm willing to share this information." I think we've gotten passed a lot of the turf issues of, "This is mine, and you can't see it and I'm never going to share this information with you." Because people are starting to realize that for the good of the company, for the success of all, we've got to share this information for us to be successful as a team. I think teaming has come a long way. I think it's gotten a lot better. So within project to project, I think we really are sharing more and I think it's appropriate, but it has to be shared at the level of appropriateness for people to jump in there and make contributions.

KL (29:49): And now, a word from our sponsor.

And actually we have the sponsor on the phone for this, our cybersecurity episode. Essential Assets Group, founded and managed by Alison Gonzalez. It's a training organization and Alison was key in pulling together our experts for today's panelists, from her pool of advanced instructors. So Alison, tell us a little bit about Essential Assets Group.

Alison Gonzalez: Sure, absolutely, thank you Kendall, I appreciate it. We have a group of premier specialists, instructor consultants, and we work with them on different client initiatives, mostly training.Training from a knowledge-based perspective or a certification-based perspective. Also sometimes on the niche consulting services side, mostly in the areas of assessments. Security assessments, risk assessments, cyber assessments, training group gap assessments, or even organizational and individual assessments.

I really try and bring people who have expertise in different people, processes and technologies aspects. They work across understanding the people from a technical competency and professional skill set, but each organization is different, and they're going to have different regulations and perspectives, so they need to keep in mind…being held accountable is a big one

KL: And that's where we step in as PMs, and that's what our podcast is about today, PMs, is the fact is, we are accountable as people at the forefront of the virtual teams, the teams that are sharing information. So thank you again, and thanks for making this happen.

AG: Sure. For more information about us and our partner network, you can visit our website, essentialassetsgroup.com, and you can also give the call at 571-418-8570.

KL: Excellent, thank you again. And now back to the round table.

KL (31:45): Organizations now are expecting people to work much more collaboratively. They're being trained for it. It's being introduced earlier in schools. It's being introduced in the technical level of training, Project Management Training, but I'm wondering how much we're over sharing on projects.

SP: I think that the collaborative communication is great. I think where I see the failing is like, "Oh

I'll just throw that on Dropbox." And I'm like, Okay, so to me when I put something on Dropbox, that means anybody that I know, don't know, could actually get it, and if I'm okay with that, if it's a picture of my dog, that's fine. But there's a lot of stuff I'm not okay with that.

So that's where you need a secured site. And I think that what I've seen with collaborative tools, I like that you can have a place where you can meet and talk, you can have a place where you can chat, you can have a place where you can, instead of having a bunch of emails in your email system, you have an email, kind of space inside of that collaborative tool.

What scares me is when you're sharing files and I'll give you an example. I was on a federal contract and we're using SharePoint to collaborate and somebody was new in the project, they didn't quite have access yet, they didn't have an account. And so somebody's like, "Oh, I'll just email it to you through your company email." And I'm like, "No, don't do that." It was like the risk register for this major federal project. And they're like, "Oh but it's through the company email." And I'm like, "Okay, so what if the email for the company gets breached?" And they're like, "It's not likely to happen." And I'm like, "And if it does well, I'll be reading about it in the front of the paper tomorrow morning. Please don't do that. Please don't send the federal government's program risk register through the company email. And I got these weird looks and I'm like, "Are you kidding me? Do I have to actually explain why that's not okay?" And I actually did. I had to actually explain why that wasn't okay. That's scary.

KL: But isn't that how we're being trained to act now? That's the thing, I don't think we think about it so deep. So I'm wondering if it may be scary, but I think that may be the requirement from a project manager's perspective is to set behaviors.

SP: And this person I was talking to was sort of on the program management team. If I was talking to a software developer, I guarantee you, I wouldn't have had to convince them of that. Because it does depend on your role. Software developers are constantly thinking, How could somebody break this? How could somebody ruin this? I don't know many software developers that are not IT security-minded, but I know a lot of project managers that aren't. They're like, "Oh I don't have to worry about that. We have a security department. They'll take care of that." And Chucks laughing in the background.

KL (34:31): I think we're getting down to what a project manager has to see. Because you have so many different kinds of people on large projects, right? From people, maybe involved in marketing, people involved with different aspects of the product that's being developed.

CM: Yeah, so I think Susan's absolutely right and that's why there should be, in my mind, there should be a security resource on every project that comes along, and that security resource, frankly, I hate to use these terms, but that security resource has to be the voice of reason about what can be shared, and what can't be shared.

So Susan talked about files, and absolutely right, you don't put it, and we talked about it, and you talk about it on security awareness, and you talk about it when you do identity management. It's the need to know. Why do you need to know this information? Need to know, need to have, need to use. So within the project, why do you need to know it? Why do you need to have it? And why do you need to use it?

So when you go through these things, and I've done this before, tell me why you need it. And I went through a company when we tried to do identity management, as an example, they were an old Mom n Pop shop, and they shared everything with everybody. Well, as they grew and grew and grew, and we went through 800-171, the unclassified controls requirements for contractors, it's like, "You don't have that; you can't have access to this anymore."

And then you kind of get into this moral dilemma or the socialization, where they sit there and say, "Well, you don't trust me anymore. You trusted me with this data for 15 years, I worked at this company my whole life. But you don't trust me enough anymore for me to have this data." And you sit there and say, "Within this project," (because our project is actually implementing 800-171: Control of Classified Information) was, "No, it's not that we don't trust you anymore, it's the fact that you don't necessarily need to have access to this information to do your job."

But as I talked about earlier, it's the socialization kind of things within the company that sometimes have to be addressed on security awareness. Why can't I have it? Well, because under these controls, it's just not going to be there.

Project managers should inject cybersecurity people, information system security officers, into every functional area, sitting at every SDLC meeting, every Software Development Life Cycle meeting. Here's our new project. Here's what we're going to do. And they are responsible at that point for helping the business owner understand what they're bringing to the table, number one. What their whole project was going to do, number two. And what that impacted the rest of the company. I want this, I want this great application, it's going to do whatever. But it's going to open ports and protocols that we don't allow.

So then you kind of go back through this and you get that early, as Susan was saying, we try to get it really as early as we can in the project, and that way we're not at the 11th hour saying, "No, you can't implement it. You're not getting authorization to run because it doesn't meet the security controls."

CM (37:28): So within the project management community, that's where you have to start talking to people, that's where the communication skills come in. That's where the sharing comes in. It's like security is always…magic, it's not magic, it's not magic, at all. It's trying to take a look, to say, "What do you need? What do you need to know? What do you need to use? When you need to have it?" And then how are we going to make sure that you…when we're done, that we've cleaned it up.

KL: In some cases there are products we're delivering, there is a role for security or things that have to be checked before it goes out the door. That needs to be part of our project planning. And Susan, you talked earlier about, don't bring them in late, bring them in early. I imagine that there's some level of awareness you're having to talk to where we're needing to put it into the project plan itself, activities and duration

SP: Yeah, they're actually... Those security requirements are requirements for the project. Remember, the customer says, "These are the requirements that I have. These are the features that I want." And then there's the scope. The scope is actually the work you do to support delivering on those requirements so that may include some security things that weren't explicitly stated by the customer, but are inherent to it.

So for example, a customer is not going to say, “I want a three-factor authentication for login.” Right? But they're going to say, "I want a secured system. Here's the data that's in there.” And then depending on the organization that you're in, if you're in the federal government, there's regulations for that that say this is what authentication you need to have for this type of data.

So that's where that scope comes in, and that's why they really are requirements, they are IT security requirements. And I think that that's the failing is if we're having that be the last thing looked at. That isn't the place for it. They actually are requirements. They should be planned for and dealt with, and even in Agile they should be on your product backlog, and they need to be prioritized based on the value they deliver to the customer. And the customer needs to be a part of that conversation to understand the value of that.

I wanted to say something about what Chuck said there before, about people having access to data. They don't need. I have a physical security example of that. So I was in an IT space, with the Federal Government, I was a contractor working there, and there was actually a hardware location, a physical hardware storage area. And somebody asked me, because I was working on a project, they said, “Well, we can get you a key to get in there, so you have access to that hardware.” And I said, “No, I don't want it.” Because here's the thing: If some item is missing there, guess what? I get a good talk-to, because I have a key, I don't want to a key to that. And we need to think about that responsibility-wise, as project managers, as project team members. If you have data, you then have responsibility to it.

I'll give you another example. The Census Bureau at Department of Commerce, whether you work there as a federal employee or a contractor, you take an oath that says that any data that you have access to, you will protect for the rest of your life. Okay? Not five years after you work there. Forever ever ever.

KL (40:43): It comes back to what Chuck was telling us about the business owner having to decide what the value of the actual information is, and therefore what the controls are. We need to remember that it's the business that owns the horse, right? The security professional is telling us what the fence needs to look like, and what could come across the fence.

What are some of the challenges you're seeing from an organizational perspective? We’ve heard from a CISO. We're hearing from a project manager what they need to be doing. What is the industry saying has become a challenge in implementing this framework and the controls related to it?

NZ: The industry's biggest challenge is insider threat. That's the biggest area of their concern. How to manage your employees, how to make sure they don't do something illegal, whether knowingly or unknowingly on social media, because the biggest breaches that we've had. Just about all of them have been either negligent, by someone inside, or someone who purposely did something because they had access. So that is the biggest issue that they have. And sadly, no amount of technology is going to protect against that. So that is the biggest challenge

KL (41:59): When breaches happen, what is it that you face from your perspective as a CISO? In terms of communicating to the project managers, what would they need to focus on?

CM: So I've been through a few breaches. One of the things that we go back to a project manager,

we would go back and say, “This is maybe within the project where we didn't take a look and get the requirements right. Maybe we didn't get the protective requirements right.” And I think the challenge is, when you've been breached, the fingers are just pointing, it’s just all out protect yourself and protect your turf. So when you've gone through a breach, they're always looking for who screwed up. Who's a bad guy? Who made the mistake?

And quite honestly, lots of times it could have been a short-change of a project. Or we recommended these controls as protection strategies, and the business owner said, “No, I'm not going to pay for it, I'm not going to do it. I don't believe that they're important.” Or you'll get this, “Gee, what's the worst can happen?” I’ve been through a couple of breaches where I've actually sat there and said, "Okay so now you've seen the worst that can happen. How are we going to fix this now? We gave you the strategy. So here's what we need to do.”

We've got to get away from whose fault it was. So for me, I go back and look at what is it that happened and what is it that within the project, maybe we could have done differently, maybe within the security controls we could have done differently? What step did we miss? Or did we miss anything, and the environment just became looser along the way, or there was a zero-day exploit that nobody knew about that happened.

You are going to be breached. It’s not a question of not happening. It's going to be when. So you got to go back and say, "Alright we own this. We collectively own this. Something we didn't do right, or something, maybe we did everything right, and we still got breached.” Okay, those are going to happen. So within the project, maybe you go back and say, “Maybe we missed a step in the project. Maybe we didn't do a good enough authorization to operate. Maybe we didn't do a good enough risk analysis. Or maybe our decisions around controls were flawed.” So that's what you have to do when you've been breached.

KL (44:06): Susan, I remember you speaking before about Failure Mode and Effects Analysis. This FMEA approach, right? What if we thought about what could happen before it happens, in the sense of the actual steps of things occurring? Where will these types of breaches happen? And more specifically, going back to what Nima had said is, it's often the insider, it's the inside problem, right? So what is it that we could speak to there as project managers? Again, it strikes me as behavior, but what would you highlight for people there?

SP: There's something actually called a pre-mortem. And then Agile has their own rendition of this called My Worst Nightmare. It's a little bit more...

KL: Oh! Plainspeak!

SP: Yeah, a little more of a fun approach. As a team member, what would be my worst nightmare for this project? And that worst nightmare could be after it's in production and the worst nightmare could be a breach.

I can tell you I worked with a lot of federal data, where we sat down and talked to the development team, and me as the project manager, sat down and talked about, “What would our worst nightmare look like?” And it always was something on the page of a newspaper and us applying for jobs at Starbucks. So the pre-mortem, it sounds bad when you talk about it that way, but I think that there is something too. We need to be okay with failure. Because if we're okay with failure, then we can talk

about it. What would it look like to fail? And then we can do something about it. So I do think that that's a cultural shift that needs to happen. The other thing, I agree with Chuck, when something does happen, it's about blame. But here's the thing. Let's say somebody clicked on a link that they shouldn't have, you could blame the person who clicked on the link. But you could also blame, Why did we not train people around that?

I teach at a few different universities and some of the training that actually occurs, they will actually send out phishing emails that are generated by the IT department. And if you click on it, they'll say, "We got you! And now you've got to go to training." I think it's wonderful, I think it's perfect. Because reality is eventually you're going to get a phishing email, so why not get one from the university that's benign, that can send you back to training so that you don't click on it next time?

KL(46:30): So what's next? What are we seeing, is the new ways we need to be heightening awareness, handling how organizations talk about security? And in fact, Nima, to you, what's coming next in training? What are you having to adjust in what you train or how you train?

NZ: I can't say what I'm anticipating honestly, because what I'm seeing happening is that training is becoming more and more, shall we say, commonplace. But the issue is that these trainings are extremely fast, extremely compressed. So instead of doing a training which is ongoing, where people attend on a regular basis, maybe four times a year, they've taken the approach of , Well we'll just send them to a three-day training, or five-day training session, and then that should do it. And if they get one of these certifications to go along with it, then all the better. Not realizing that that really doesn't protect them. They're happy to get the certification, and government nowadays is putting money on this. So I had a bunch of people who said, "If I pass my Security Plus I get a $10,000 raise where I am. So that's what they were there for.

And all of them passed Security Plus, because it wasn't that hard to pass. But that doesn't mean they know anything. So that's unfortunately the trend right now. That's where it's going. Until there is…and I don't know if it's going to happen, but a fundamental shift that, "Listen, this is now how this works."

You need to have regular training. Quarterly is my recommendation. Where everybody has to attend. And you don't have to go through everything. You can go through, you know, divide up your security into four pieces, and four times a year, you go over one quarter of the security requirements. And it becomes part of the company culture, or part of the government agency culture.

Until they do that, they're going to have issues, they're going to keep having issues, more and more, because the problem is not technology. We have the technology, we have good coding. The problem is two-fold: One, people aren't aware; and two, they're too cheap. Like Boeing hiring $9.00 an hour, Indian programmers to do their codes. So those two need to be addressed.

KL: So we've got to be able to evaluate the price of the horse, and actually how much the fence costs. So Chuck, what are you seeing next as you're consulting in training and raising awareness yourself?

CM: So one of the things that I'm seeing is there is always, how should I say, two different levels of accountability within a training. The senior executive leadership, quite frankly, did not, in the past,

want to be held to the same training standards, and held to the same controls. And, you know, there's no personal email on the system, blah, blah, blah, things like that. So executives didn't want to be held to that. What I'm trying to see is that more and more, as executives are being held accountable for failures, they're now starting to understand that these rules apply to them as well. I'm starting to see that a little bit more.

One of the things that I saw years ago, at Department of State, was that every time you logged on to a state system and, don't hold me to this specifically, but I believe it was every time you logged on to a system, you got a security question. And you could ignore the question, I guess, three times. And then you were locked out, if you didn't… and it was weekly. It wasn't quarterly, it wasn't yearly, and we tried to implement it over at the Postal Service, and I was not successful in that because when you're dealing with hourly people versus salary kind of people, that starts to impact how quickly they get to work. So there were some challenges there.

I think there has to be ongoing…there has to be testing. Like if we do a phishing test all the time, and people do this. And we'll do phishing campaigns. And we'll do, you know, socialization campaigns. And then we do external penetration testing, and we'll try and do red teams we'll try and do blue teams, and I'm like... Yeah, and now let's do some social testing. You know, the typical Call-the-Help Desk, and saying, "Oh I forgot my password, blah blah blah." And I have enough information to become that person. But you're testing the whole system. When I was at Postal, I would have my team issue an attack, and I would let it go right to where we were ready to announce to the management that we're under attack. Because I'm checking the help desk, I'm checking my log analysis people, I'm checking my incident responders, I'm having, I'm actually testing everybody along the way. And they would come running in to the office, "Oh, we had a bad thing happen." And I'm like, "Okay, what is it that you found?"

And then when they weren't finding them, we were having that conversation as well. How did we miss this? I launched an attack on this last night from this particular IP address. How did we not see this? So I think we're going to have to do more and more realistic kinds of engagements, where we get people, Number One, acclimated to what they might see, and Number Two, sensitized that they have to have a response, what they're accountable for, working within the security awareness. I think it's more actionable as opposed to, Sit here quarterly; Read this; Watch this video. To me, that's kind of that's not getting the job done. I'm going to test you, I'm going to make sure, I'm going to make sure that you understand what phishing looks like. I'm going to make sure that you know what somebody might say to you when they're trying to get your log on ID, and I'm going to make sure that you understand how they might try and social engineer you. That's how I think we're going to get better. But I think making sure that everyone follows the same rules, regardless of their stature in the company, has the same accountability. I think that's where you'll start to really see some value of the whole training exercise, and that's the future in my mind.

KL: Secure behaviors, not just for other people anymore.

CM: Right, absolutely, it's not. And the executives have to understand that.

KL (52:27): Susan, as you're out speaking and raising awareness on this issue as part of a larger risk discussion, I think, that you often are talking about, what do you see as where you're going to want to pivot or you see potential new threats or new ways that this conversation needs to be held?

SP: So what I see is that as project management professionals, we are being asked to do more. First we were asked to understand our customers better, to understand business value better. Now we're being asked to take responsibility for IT Security. So project managers are, it's just another thing that we need to be knowledgeable of, at least in a small degree. Project managers will ask me and they'll say, "Okay I got it. I need to know about IT Security. Now, how do I do that? What certification should I get?

I don't think there is a certification out there right now. So this is sort of…PMII should be listening. I do think there would be some value to have some IT security training that is geared towards project managers. What can they be aware of so that they can make sure as a Project Manager, they're doing the right things, and they're getting the right subject-matter experts involved early on in the project, and that doesn't exist. PMI has a risk Management Professional certification, but it's not focused on IT security, and I do think that everybody needs to be more aware.

The social engineering thing. I'm glad you brought that up, Chuck. Another thing that technology does not fix. Technology…no amount of technology…is going to fix social engineering. It is actual awareness. So those types of things are really about educating people, and people being professionally responsible for that. I can tell you when I took that oath at Census Bureau, you feel more responsible when you take an oath like that.

KL: The act of priming people for proper behaviors, matters a lot. And sometimes those ceremonial kick off…the ceremony of beginning things might be a place to catch some of that.

CM: We have to look at it's not IT security. It's corporate security. Because when you say IT security, they're thinking IT is doing all this work and they don't end up with this kind of collective ownership. So IT's doing it. It's IT security. It's just like it's IT privacy or it's accounting privacy. No, it's corporate. And it has be looked at as corporate. It's a corporate collective. We are all responsible, we all own the enterprise. Security is great. I have…something like that, because when you say IT security…people saying IT owns this…whereas everybody owns this. So I spend a lot of time on the soft skills today, getting people to understand how important it is to be collaborative, how important it is for the partnerships to happen.

You don't do security, for the sake of security, just as you don't do technology for the sake of technology. You do it for the benefit of the business, for the benefit of the customer, and to support the mission statement.

KL: Project managers are broadly managers, and they may not be doing only IT projects and they don't interact only through IT as well, right? They are part of the our corporate effectiveness. Yeah, fair point.

CM: We need to make sure that people understand they have the ownership of this, as a collective. It's not a functional issue, but a collective issue.

SP: Project managers don't have to be cybersecurity experts or IT security experts, to be aware of the cybersecurity concerns that every project has. And I do think almost every project has some elements of that, and definitely every IT or software development project does. And basically, if you're not doing risk management, if you're not managing your risks, then you're taking them, I think that this is an evolving part of project management and we need to grow and learn. Get on the

train or be left at the station, so don't be left at the station for sure.

KL (56:33): Take heed, project managers, lest you get left behind. The cyber problem is endemic now for any of us knowledge workers. It is not a matter of if, but when, you, your team, or your organization gets hit. In this rapidly changing environment, ongoing continuous training is important, and recognizing the threat and addressing it right up front at the kickoff meeting and during project initiation is key. I know we get told to communicate, communicate, communicate, but the overriding managerial safeguard for your information is to limit its circulation. Not everybody needs to know all the details of your project.

And I know that feels wrong, it contravenes so much of our training. But remember, whether it's deliberate or inadvertent, insiders are often the culprit. We are all responsible. We must all hold our stretch of the Line of Defense.

Special thanks to my guests, Chuck McGann, Susan Parente, and Nima Zahadat. You can reach out to Chuck and Susan via LinkedIn. Nima can be contacted at captainnima@hotmail.com. That's Nima N-i-m-a. This episode was sponsored by Essential Assets Group. And again, I would also like to thank Alison Gonzolez for making this panel possible. Alison can be reached at alison@essentialassetsgroup.com. That's Alison with one L.

Announcer: Our theme music was composed by Molly Flannery, used with permission. Additional original music by Gary Fieldman, Rich Greenblatt, Lionel Lyles, and Hiroaki Honshuku. Post-production performed at M Powered Strategies.

KL: PMPs who have listened through this complete podcast may submit a PDU claim, one PDU, in the talent triangle Strategic, with the Project Management Institute's CCR system. Use provider code 4634, and the title "PMPOV0067 Cybersecurity in Project Management." You can also use the PDU claim code 4634UKD1P2.

Be sure to tune in to next month's episode, our third in the series from the University of Maryland's 2019 Project Management Symposium. This one focuses on project management in the federal government.

Presenter A: We have projects that go on for a long time. We're not for-profit. It's more about doing the right thing for the greater good. It's ownership and long-term stewardship, as opposed to perhaps in the private sector, where itt's jumping for one to another.

Presenter B: So those of you who are feds, or have been feds, know the term Do More with Less. And so we're trying to figure out new and innovative ways that we can streamline and make the best use of our resources, but also make the best argument from a risk perspective, for the resources that we do need.

KL: Visit our Facebook page, PM Point of View®, to comment and to listen to more episodes, and get the transcripts. Leave comments on PMI's, projectmanagement.com portal – I like to read those. Evaluate us on iTunes, and of course you may contact me directly on LinkedIn. I'm your host, Kendall Lott, and as always, keep it secure, keep it in scope, and get it done.

Announcer: This has been a Final Milestone Production sponsored by M Powered Strategies.