33. Pelletier, Sears & Tobin: Security

0:00:01 Kendall Lott (S1): Hey, PMs. We've just launched a Facebook page for this podcast at facebook.com/pmpointofview, all one word. So in addition to all the other sites that you can get this podcast from, you'll be able to listen to our podcast from that Facebook page. And more importantly, we invite you to leave your comments. We will also post information about our guests and content from our guests, so like our page and be part of the project management dialogue.

0:00:27 Paul Pelletier (S2): You can see how if you take your lens and broaden it, how much project management actually is fundamental to the success of our justice system.

0:00:38 Dave Sears (S3): No matter what you do and what you plan, the minute the first bullet goes down range or the minute you begin executing the plan, you're deviating. It never sustains first contact.

0:00:50 Chuck Tobin (S4): Metrics are a very challenging mark point for our industry, because no news is good news.

0:00:58 S1: Today's environment of high crime and terrorism has all of us on edge. Whether it's domestic or international, real or imagined, in the air, on the ground or in cyberspace, the need for security is real and it's on the rise. As the requirements increase in complexity, we see project managers playing a crucial role. In this episode, I spoke with three experts coming from three different perspectives. Justice, law enforcement, Homeland Security for national security, and private security. We talked about the details of their profession and how project management can bring about better results and greater security.

0:01:33 Speaker 5: 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's your host, Kendal Lott.

0:01:44 S1: Paul Pelletier wears many hats. He's a project manager, a corporate lawyer and a former business executive. He writes, conducts webinars, is a sought-after speaker and also happens to be one of the recognized influencers in the projectmanagement.com portal for PMI. A native Canadian, Paul spent over 10 years working for the Department of Justice of Canada and is an enthusiastic proponent of project management in crime scene investigation. Yeah, that's CSI. That sparked my interest, so I reached out to him via Skype at his home in Vancouver, British Columbia.

0:02:16 S2: Project management, unbeknownst to many of us in the profession, actually has revolutionized criminal investigation and prosecution by providing structure, best practices and, most importantly, the case management system that is used almost uniformly by every first world policing department. Every criminal investigation and then prosecution is a project and it involves a whole team of people with various investigative and legal skills. And the impact and intersection of project management with major crime scene and prosecution is real. And if we think about it, what

does crime scene investigation need? Meticulous attention to process and details, incredible capacity to very carefully and consistently compile and maintain evidentiary and information management.

0:03:15 S2: And it's driven by precise methodology and painstaking project management techniques. So, when we back up, we realize that in order to successfully prosecute somebody, we have to be able to lay down a case with extraordinarily meticulously presented evidence and witnesses and often we have to deal with not hundreds, not thousands, but in major crimes, tens of thousands of pieces of evidence, whether they be wiretaps, whether they be film, whether they be computer records.

[music]

0:04:00 S1: If I'm watching TV, the detectives are out gathering that stuff, and there's somebody else doing analysis, but you rarely see someone sitting in the center of it, and certainly monitoring the process. So clearly, that's probably not so sexy, so they probably don't show it on TV.

0:04:15 S2: It doesn't make for glamorous and exciting TV to see someone sitting behind a computer organizing thousands of pieces of data. But that's exactly what happens. So there's a system that has been designed for incorporating project management into criminal investigations, and it's called major case management.

0:04:37 S1: Okay, let's back up here. Among the tragic series of events that led to the development of major case management and other similar methodologies designed to help criminal investigation, there was the disastrous Air India flight, which departed Montreal, bound for London, in June of 1985. It blew up in mid air off the coast of Ireland, killing all 329 people on board. To this day, it remains Canada's worst terrorist attack ever.

[music]

0:05:05 S2: Let's go back, 1985, no computers, no capacity to communicate rapidly, to share information easily. It was an absolute nightmare to try to get organized all of the players. So we had stakeholders in India, because we were trying to get suspects there, stakeholders in the UK, 'cause two of the suspects had fled there and needed to be slowly, but surely, extradited, and we had the equivalent of our CIA, we had policing forces, we had government departments, we had... Everyone who wanted a territory and everyone wanted to control.

0:05:47 S1: So, is this a problem of who owned it or rather who got to execute the process? Sounds like a stakeholder management problem.

0:05:53 S2: It was just an awfully complicated mess, and we had no tools and no structure and no methodology. So the sad result is the case lasted 20 years. It wasn't until 2005 that the first court verdict was obtained, and ultimately Canada only got one conviction for manslaughter when 329 people died. It was the most expensive CSI and trial in Canadian history. It cost $138 million. And afterwards there was a government inquiry, because the result was so unacceptable to the society, that the inquiry ultimately said that there was a cascading series of errors.

0:06:36 S2: But what was learned is that CSIs have to have an over-arching project management

structure, and PM technology has to be integrated into complex CSIs. Improved information management is needed, better resource coordination, better investigative excellence and improved police training. So what happened as a result of this horrible event, we got the first over-arching PM strategy for CSIs and customized PM software in the form of this Major Case Management System.

[music]

0:07:14 S2: Within that major case management system there are roles where you may very well have a senior investigative officer who is in charge of some aspects of the investigation. But you're gonna inevitably to have someone whose role it is to compile all the information in a strategic and concise and consistent form and to do the Gantt chart work. Which comes first, where? What type of evidence needs to be compiled in what form? And so on. That information is documented and managed using a set of administrative procedures. And it's put into a system that is used by the senior investigating officers. But it is a critical project management tool and it's really like agile for those of us in the field of project management.

[music]

0:08:19 S1: Does the case management tool allow us to coordinate better with stakeholders?

0:08:24 S2: Well, of course, because there is a stakeholder management plan incorporated into it. And so there are, just like any other intelligent project management plan, it incorporates a communication plan, a stakeholder management plan, a risk management plan. All of these components, they may not be called that, but that is what they are and that is what they do. So each of the project management disciplines have been incorporated into major case management. I didn't even appreciate just how integrated it was until I saw it coming out of the mouth of a police investigator and realizing, "Wow, you're just talking about stakeholder management plan. Oh, my gosh, that's a risk management plan. Hey, you've got a work breakdown structure." You might not call it that, but that's exactly what it is. And they use Gant charts. I've seen one. So, wow. So, police and Gant. Did you ever think that would happen? But it does every day.

[music]

0:09:31 S2: Now the police as a whole, and certainly legal work as a whole, has been a late adopter to actually engaging project managers to do this work. However, I can tell you that that's changing. And it's changing quite rapidly. There are police forces that actually have roles, permanent roles, for project managers. And certainly in the context of legal work, court administration and the work that is done by law firms and by departments of justice, there are roles absolutely for business analysts now and there are roles for project management professionals.

0:10:12 S1: You're saying a person trained as a project manager might be able to be attached to a large police department?

0:10:18 S2: Absolutely. When I presented at the Dubai International Project Management Forum on this topic of the intersection of project management and major crime investigation, we had the absolute honor of being able to tour the Dubai Police Facility and they actually have full time project managers doing this kind of work.

[music]

0:10:49 S2: Let's talk about project management and the PMBOK for a second. Within case management, you have a project management methodology and system. You have stakeholder management, 'cause you've got all the witnesses, the victims and their families. You've got the press, you've got society as a whole. You've got the defense on the other side of the table. So you've got all of those stakeholders that ultimately they want to see justice done. But you have to do all the right work to get it done. And then you've got resource management, 'cause you've got all kinds of talent doing everything from blood splatter analysis to computer programming and taking out hard drives. And then you've got risk management, whether it's legal risk or whether it's project risk. So you can see how if you take your lens and broaden it, how much project management actually is fundamental to the success of our justice system.

[music]

0:11:54 S1: This is really interesting to me as I've looked at other industries and their use of the project management discipline, I'm often struck by which parts of the PMBOK is most important or most sensitive for their needs, right? Stakeholder management, scope management, etcetera. Quality is the highest problem here. You've used the word meticulous about three or four times now, I think.

0:12:12 S2: You got it. It doesn't matter how good your evidence is, it doesn't matter how slam dunk of a case you have, if you can't present it well in a methodical, laid out, very well-managed process, then you're gonna have a whole lot of trouble convincing a court or a judge to rule in your favor. Interestingly enough, this exact issue in the United States, in particular, thanks to the new television series on the OJ Simpson trial, this has been highlighted. Because they had all the evidence in the world and they had all of the information they needed to convict, but because the information was not well-presented and it was not well-documented, we saw a result that I think uniformly we can say wasn't the right result.

[music]

0:13:08 S1: We're seeing it now embedded rather deeply, is your suggestion here. And is that at the national police force levels? Where is this discussion happening?

0:13:18 S2: Well, it's happening I think at every police force. And we all know just how sophisticated criminals are and how sophisticated the technology that they can use now is to achieve their really terrible results. So we, I think, as society and the police in particular, have to somehow meet fire with fire, and I think that's why police forces are realizing that in order to do the job that needs to get done, it isn't just about policing. It isn't just about being a cop on the street or investigating a murder or a major crime, but it's also about how that evidence is managed and how that information is managed, and how the team is managed and how you've got your work breakdown structure, and your Gantt chart. All of that is now being incorporated. It has every element of the PMBOK definition of a project in it. They're temporary, they have a definite start and end date, they produce a unique product or service, and they're complete when the goals are met. What other part of this do we need to look at when we're categorizing CSI work as projects?

[music]

0:14:36 S1: As soon as you've made this a project, it seems like that immediately starts screaming portfolio. I'm the head of a police department, so I'm wondering, "Am I getting the best return of all of the cases I'm entering?"

0:14:49 S2: No question about it. And I don't see any reason why police forces should not be talking about ROI, return on investment. 'Cause what do we want? We wanna see justice served. And if bad people do bad things, as a society, we want them to face results of their actions and accountability. So if our our investigative reports that come out of our investigation are as strategically brilliant as they can be, undoubtedly, we're probably gonna get better results.

[music]

0:15:29 S1: I see a new horizon of opportunity here. What would happen if a PMI Chapter teamed up with a local police force offering free training, or a support for certification, or even support for methodologies to be used by the police force? Think what we could accomplish.

[music]

0:15:53 S1: My next guest, Dave Sears, is a retired Navy SEAL Commander with 20 years of service. He started in basic underwater demolition training, and worked his way up the ladder, ending up at corporate headquarters for a special ops command. A decorated veteran, Dave planned, led, and executed hundreds of special operations missions in more than 40 countries on five continents. He's currently a managing partner for Xundis Global where he does consulting for national security organizations, security firms and cyber firms. I wanted to pick his brain about special ops, and how missions can be approached as projects.

0:16:26 S3: So we have joint publications that are the PMBOK. So you have a joint publication 3-05, joint special operations, task force operations. So it's...

0:16:39 S1: The guidebook.

0:16:40 S3: It's the guidebook for conducting operations. And there's another one called joint publication 5-0 code that's a joint planning process. They have very, I mean, they go down step by step, and people reference it all the time.

[music]

0:17:01 S1: How could you even begin to frame any of the operational type of things that you've seen and worked with as a project?

0:17:07 S3: Okay, let's talk about three levels first, and they all look like projects.

0:17:11 S1: Okay.

0:17:12 S3: You have a strategic level, guidance may come down. It may be from the National Security Council that says, "Here's the National Security Statement. This is the posture that we're gonna proceed with." Then the Pentagon develops... How is Department of Defense gonna execute

this guidance and our security posture? We see Russian aggression in Europe as a threat. What are we gonna do for a strategy to counter that Russian aggression? And now that goes across the entire inter-agency, governmental community. So how's the Department of Defense gonna handle this? How is the intelligence community gonna handle this? And how is the State Department gonna handle this? And you try and mesh all those together. That's at the strategic level.

[music]

0:18:01 S3: Then you'll start to take operational pieces, so there's an operational planning level, which is the middle level. It's almost a giant project charter. So if you think about projects nested in projects.

0:18:16 S1: Sure. This about alignment. There is that strategy at the highest level from the executive level that is dealing with what does the future look like? And then that devolves into portfolios of projects and those are wrapped up in programs, but you eventually get down to the projects that actually are where the work happens.

0:18:33 S3: Right. So now you get into that tactical where you have much more defined states that are, "Here's the beginning and end". I will get a tactical mission. We have this intelligence that says there's a suspected terrorist, he's gonna be on this ship at this time. I need you to go capture that guy.

0:18:50 S1: So you have to make a plan?

0:18:52 S3: So now I gotta make a plan, and you start back with...

0:18:54 S1: And the clock is already running.

0:18:56 S3: The clock may be running. You may have some things that are preplanned that I want you to be able to do this in the future, develop made plans that you put on the shelf. So we do a lot of this that I don't think exists as much in the PMP world.

0:19:09 S1: We do a lessons learned sense of if you've done it before and you figured out what was good or bad, you keep the past performance, the past examples. But that's a little different than what you're suggesting, which is some time to say, "Go ahead and mock up 80% of the plan or 40% of the plan."

0:19:25 S3: Mock up a plan and put it on the shelf. And that tends to happen at the operational strategic level more than the tactical level.

0:19:31 S1: Keep us at the tactical level.

0:19:32 S3: So at the tactical level, now I start to do a feasibility assessment. So I look at it and I go, "Okay, what you've asked me to do, can I do this? Is it possible?" And I start to envision my charter and, "Okay, what is this gonna look like? Is this even in the realm of the possible?"

0:19:52 S1: When you ask that question about possible, is that technical possibility or is this fundamentally a budget resources possibility, or are you already wrestling all of that at this point or do you suppress some of that while you're trying to address another part of it?

0:20:04 S3: No, you're doing all of them at the same time. So I have to look and say okay, "Do I have the resources to get here and do this?"

0:20:11 S1: You're asking that question right out of the gate?

0:20:13 S3: Right out of the gate. So there's one model that some people use. Is it suitable, acceptable, feasible? So suitable is the course of action and the plan that I'm developing, does that meet the requirements that I've been asked to do? Is it acceptable? Does it fall within the values and ethics and norms, my course of action that I'm developing for this? I need to take out that terrorist. Okay, let's drop a nuclear weapon on them. Okay, that's not acceptable, it's not in general within the norms that are established.

0:20:53 S1: So there're some sense of ethics or professional requirements or basically it's constraints from outside stakeholders in a way?

0:21:00 S3: It is, it can be absolutely. Yes.

0:21:01 S1: Okay.

0:21:02 S3: Then is it feasible? That comes to the resourcing piece. Do I have the resources to do this?

[music]

0:21:09 S3: That feasibility study first tells me. I get a general look, I say, "Yeah, this is within the realm of possible, certainly." Now I start to do a mission analysis of that. And then from that mission analysis I'll flush out more and I'll say, "Look these are starting to look like the requirements." I'll list out and say, "Here's the limitations that are placed on me," I'll start to there figure out what's my, we'll call it friendly situation? So I'll start to really look at the situation...

0:21:38 S1: So you're doing some scenario analysis, and you're documenting constraints?

0:21:41 S3: Yeah, absolutely. You're doing constraints and limitations. You're putting in there what are your assumptions? What am I assuming is gonna happen, what am I assuming I'm gonna have? I write in my constraints, my limitations, I'm gonna do a stakeholder analysis to an extent. What do my bosses want? Who all is involved in this? Who am I gonna have to bring in from the outside? Do I have to use intelligence agencies? Do I have to go through an embassy? So I'm gonna be crossing the borders of another country. They're a stakeholder in it, are they witting to this, are they not witting to this? They're still a stakeholder, the same with what commands and what pieces of the business am I gonna use. So the stakeholders are the operations department, the stakeholders are the intelligence department, the logistics department, all these things, then I start to look at the enemy, the pieces that I don't get a say in. From there, I go back and go, "Okay, here's all the things that I've figured out about this." Then I will develop a course of action.

0:22:46 S1: That sounds like a charter right there. It's like, "I'm gonna need these things to do these things".

0:22:51 S3: It's right in between I think a higher level of the charters written and then I'm writing a more refined view of that charter.

[music]

0:23:04 S1: When do you bring in colleagues, or do you?

0:23:07 S3: Always.

0:23:08 S1: So this is a collaborative thing from the beginning?

0:23:08 S3: It is collaborative from the beginning.

0:23:11 S1: So you got a team kind of tossing in the ideas and getting it done?

0:23:13 S3: Yeah, exactly. What I'll do is I'll get the mission, and my boss will assign it to me and say, "Here is what you need to accomplish." The next thing that he wants to see is he may want to see my mission analysis of how I broke it down and who all these players are and everything in there. The next piece that he's gonna see is what are my courses of action. And that gets into the nitty gritty of how am I gonna execute this?

[music]

0:23:43 S1: When you get these to get started you're given the outcome though, right?

0:23:46 S3: That's not an open-ended question, no.

0:23:48 S1: It's the how you're going to do it.

0:23:49 S3: But in the feasibility I can come back and I can make suggestion and say, "It's not feasible for me to capture this guy."

0:23:57 S1: In this way with...

0:23:58 S3: "Do I have the authority to kill him?"

0:24:02 S1: So there's a bit of a design element happening in your feasibility.

0:24:05 S3: They can say something like, "Hey, we want you to bring back 50 people." I go, "Look, the resources here and there and the constraints and the scope that you've levied on me, say you want this to be clandestine. You don't want me detected, to some extent, you want me to use these limited resources so I'm not taking an entire army in there. I'm only taking four guys, eight guys, 16 guys. You want it below the radar, but you've told me to pull out 50 people. I can't do that without bringing in a whole airplane and giant trucks. So here's my recommendation as what... " Then I may have a dialogue on, "What's your intent to this? Do you just want two or three people that I can pull off and we can gather more intelligence from?"

0:24:53 S1: This is another thing. As we're going through, I'm flagging things that possibly project

managers could be learning from your environment. What I just heard there was the project manager having a voice back into before we've completely engaged in this, what this may need to really look like. Is the documentation then something that is important, continues on? Is this part of an audit trail?

0:25:20 S3: All these are time-dependent, especially in the tactical world. So I may have opportunity to pre-plan a target. I might know one month out this guy is gonna be here now, I'm gonna go through a much more formalized planning process. When you get down into it, there's a way that they can tell me to go out of scope and this is called a frag order, fragmentary order. So while I'm in the middle of this, I'm getting ready to assault this ship.

0:25:53 S1: So execution? You're past planning, you're into execution?

0:25:55 S3: We're past planning. We're into execution and I'm in place getting ready to assault this ship and I get a call that says, "We just got new intelligence. There's a higher level guy over here that we want you to go grab him or we want you to execute this, but now we've changed. When you grab this terrorist, we need you to go to the next ship over and grab that or we need you to blow up that ship on top of it." I'm like, "Okay, now I've had a change in my original plan of scope." Now, when you get that fragmentary order, during execution at some point or right post-execution, it'll happen a lot of times, I think that I've hit my end state.

0:26:33 S1: You think you're done.

0:26:35 S3: You think you're done, you're not done.

0:26:38 S1: The frag order looks like a change management request, or a change request, I should say.

0:26:41 S3: Yup, that's it.

[music]

0:26:48 S1: Is there in fact oversight in governance? Is there some way somebody knows how this is for you...

0:26:52 S3: There is.

0:26:53 S1: When you're done or doing or anything.

0:26:55 S3: Yeah, absolutely.

0:26:55 S1: And how does that play into your world as the project manager of this project?

0:27:00 S3: So just like project management, I'm gonna have steps and phases in there where I have to show you. So in the planning process, I'm gonna go towards first course of action development and I have to give multiple courses of action. So I have to present my boss with... Usually the standard in the military just kinda come down to three courses of action.

0:27:27 S1: It's like three simple plans, almost. Three different sets of work breakdowns.

0:27:30 S3: It can be, yes. Here's three ways I believe to accomplish this mission. Now, there may only be one feasible, there might just be two.

0:27:40 S1: Okay. So a little bit like alternatives analysis then.

0:27:43 S3: It is, you wanna look at that. So for example, we'll break down a mission into the very simplest aspects of it. First you're gonna have insertion, then that's followed by infiltration, then my actions on the objective, then I have exfiltration from that objective, and then I have extraction and then there's a post-mission piece. So insertion, I can say, I'm going to sky dive in and we're going to land in the water. My infiltration piece is then I'll swim into that ship. Now I'm at the objective. My team will then climb onto the boat. We'll move around the boat, get this guy. We will contain him there, we'll contain other people. We tell what we're gonna do with everybody on the target. We might tie them up, restrain them, we may not, we may confine them to a room. Are we gonna interrogate them? Are we just gonna leave them? What's our timeline? And then we're going to go off onto the dock. That may be the exfiltration. We're go to the dock to a waiting cargo truck that we've arranged and we'll drive over and across the border, at which point a helicopter or a plane will pick us up to take us home.

0:29:02 S1: And that's your extraction.

0:29:04 S3: An alternative course of action might be I'm going to drive in in a truck and come onto that ship.

0:29:13 S1: So you plan these as different scenarios.

0:29:14 S3: So you plan these as different courses of action.

0:29:16 S1: And they see those in the planning stage.

0:29:18 S3: They see those in the planning stage and I go back to the boss and I present him these courses of action and then he says, "I like course of action one."

[music]

0:29:33 S1: So again, where does the governance happen as you go through this?

0:29:35 S3: So during execution, you'll have something that's generally referred to as an 'execute checklist'. So now what I'll do is I'll list out every piece of that operation. Across the chart is says insertion and with that insertion, I'm gonna have a call and I'll list on there who the call's from and who it's to.

0:29:58 S1: So it's a communications plan?

0:30:00 S3: It's a communications plan, but it's also an execute checklist, because in there there's also a caveat that can be, "At this point, I need an execute order, or I need go criteria." So he can say, "Yep, you are authorized to go through step one, step two, step three, you have to get... " And

usually this happens right prior to the objective or prior to the insertion. So, if I'm gonna cross into another country's boundaries, I say, "I'm on the plane, we've completed... " and you have, what they call pro words. So you just establish a whole checklist and it's a single word, so I say, "Cheetah." They know and they look at their checklist, and they're like, "We just received Cheetah."

[music]

0:30:51 S1: I think you're dealing with a riskier environment than many project managers experience, [chuckle] if not all of them. Tell me how you see risk, and how is that processed in the planning and execution and lessons learned phase?

0:31:06 S3: When you do have the luxury of time, you have a whole risk matrix that you go through.

0:31:13 S1: Really?

0:31:13 S3: So, let me take a different example. The same planning goes into a training operation. Let's say I just need to go to the shooting range, and I'm gonna execute some training for my guys, I'm gonna put another guy in charge of it, right? "Hey, this is your project. You set up three days of training at this range." He's gotta develop also a risk matrix, and we have a format that goes with it, and you sit and you look at, "What are my possible dangers? What are the risks? How do I assess those risks?" And those risks get assessed based on, from the gravest, to could this involve loss of life or limb. That's like the highest. Then down to, could this involve somebody being put out of duty? Could this involve damage to equipment? And he has to go down and grade this.

0:32:02 S1: Is that in order to see a better plan to reduce risk? Or is that to be able to determine potential costs?

0:32:08 S3: This is to inform us and to make sure that we're aware of the risks, but then with this risk assessment, you have to mitigate. So now you have to list, "What steps do I take to mitigate that risk?" And so here are the steps that I've taken to mitigate that risk: I'm gonna make sure that everybody's been briefed on the range procedures, I'm gonna make sure that all weapons are located in this area. I'm gonna make sure that everybody's been through at least expert marksman training, I'm gonna ensure that they've had these prior requirements before they get on the range. So I'm gonna do all these things, and now I take my risk category, and I say, instead of a Category One, which is my initial risk without my mitigation implemented, now with my mitigations implemented, I'm at a Risk Category Three.

0:32:56 S1: Do you have a threshold of some weighted amount of, "90% of the risks have to be a Category Three or lower"? Or that kind of thing?

0:33:02 S3: Yes.

0:33:03 S1: So you set up, okay...

0:33:04 S3: So now if you have something that's...

0:33:06 S1: And indication when to do this.

0:33:07 S3: In a high category, it has to be signed off on by a boss, senior.

0:33:13 S1: So accountability is being built into this.

0:33:15 S3: So accountability is being built in. So that senior boss says, "I understand that even with the mitigation measures in here, these risks involve life or limb, and I, as the boss, am signing off and saying that the juice is worth the squeeze."

[music]

0:33:33 S1: So we've covered here this idea that now some risk and scope schedule.

0:33:38 S3: Right.

0:33:38 S1: Talked about some timing issues, implicit in this is budget.

0:33:41 S3: Yes, that is one thing we do not have to deal with as much [chuckle] as a project manager.

0:33:47 S1: Oh, in what way? [laughter] They knew they were doing something harder than a SEAL had to do.

0:33:51 S3: Especially when you get to the tactical piece, budgets aren't as big a constraint. They're almost not even accounted for to some extent, it's already a, in the military to some extent, it's already a lost cost.

[music]

0:34:07 S1: It is my sense that if your project starts to go bad, bad things could...

0:34:12 S3: Yes.

0:34:12 S1: Very risky things are occurring.

0:34:14 S3: The consequences are much greater. So this is why we do training events. I'm not just gonna take you as a new guy, and say, "I want you to go run this combat operation, here you go."

[music]

0:34:26 S1: What does quality mean to a leader of a small SEAL team who's having to plan and execute an operation?

0:34:32 S3: Ultimately, quality means, "Did I accomplish my mission?" Which involves the one, the mission parameters I was given, and then two, did everybody come back safe and alive?

0:34:43 S1: Generally those become very clear very quickly. "We did what we said we were gonna do, and everybody got home."

0:34:47 S3: At the tactical level, very easy to measure.

0:34:49 S1: Take them to your portfolio, we got all these things going on. How do we know if it's working?

0:34:53 S3: That's a very good question. They've, the government writ large, the Department of Defense have constantly struggled with this measures of effectiveness. And they use some standard business practices on certain things. Did I stay within budget? Did I accomplish what I set out to say I was gonna accomplish? So I can say, "Okay, so I'm gonna go train these special forces in this other country on marksmanship." Well, I have, one, I have this time, did I meet the timeline? I want 80% of their guys to be able to shoot, expert marksmen, and I'm gonna run a test that says, "You're gonna shoot from 200 yards, and you have to put this many bullets into the bullseye in this amount of time.'"

0:35:36 S1: And the 80%'s measurable.

0:35:38 S3: And the 80%'s measurable. So I can say, "I had 100 guys that I trained, or I had 100 guys that I trained, 80 of them hit this metric."

[music]

0:35:48 S1: How high would MOEs go?

0:35:49 S3: They go...

0:35:50 S1: Do they set them all the way at the strategic level?

0:35:51 S3: They do.

0:35:52 S1: Oh, okay. So this is a cascading effect as well. Or a decomposition.

0:35:54 S3: It is, but at the tactical level it'll become much easier to measure. There are physical metrics that I can see. As you move on that continuum up to the strategic level, it's much harder to establish democracy around the world or have them embrace rule of law and fair governance. And you try to list under that, they'll have 1.1, they've instituted judicial reforms, 1.2, they've done this.

0:36:25 S1: But your MOEs are coming a little bit from the bottom up, so do they meet in the middle?

0:36:28 S3: They do meet in the middle.

0:36:29 S1: Do you get into an alignment question?

0:36:30 S3: Yes, exactly. So you have to be aligned with, "Okay, are these measures of effectiveness that they've established at the operational strategic level, are we nested within those? Are our things hitting those as well?"

[music]

0:36:46 S1: This is a very rigorous institution and yet you're doing very dynamic and flexible things. And is that problematic?

0:36:53 S3: It is problematic. They can collide, especially when you have this huge institution that wants to do these planning processes, yet they need the flexibility. This is especially where special operations can collide with it. No matter what you do and what you plan, the minute the first bullet goes down range or the minute you begin executing the plan, you're deviating. It never sustains first contact. So you need to understand the path that you're on in order to reorient and get towards that path when you're thrown off of it. You need to step outside of the process and think through some of these possible contingencies. So that when they happen, you're prepared to respond. Looking at the whole project, then focusing in on the piece that you're at in the current time, where you're adjusting your focal length, looking at the whole project. So you're constantly adjusting this focal length as a project manager going, "I need to make sure that I see the larger context."

0:37:58 S1: Dave recently coauthored a book with Charlie Black, one of our earlier podcast guests on crisp thinking. He teaches crisp thinking and design thinking with Charlie at Xundis Global. To contact Dave, you may reach out at partner@xundisglobal.com. That's Xundis with an X.

[music]

0:38:23 S1: Chuck Tobin is the chairman and president of AT-RISK International, a private security firm which has been providing executive protection, risk assessment consultation and investigations for clients for more than a decade. With offices in the US, Rio and Dubai as well as partnerships in South Africa and Mumbai, their primary focus is on international executive protection services and handling stalking and unwanted pursuit cases.

0:38:47 S1: So, we wanted to talk about the issues of security from a project management perspective. So, in what context can we describe a project that you might undertake, which is something where you engage in some sort of security practice for some period of time that has a beginning and then an end?

0:39:05 S4: Yeah. I would say there's two obvious project efforts, so to speak. The first one is in the grander scale where a corporation might have determined that they are concerned for the safety of their executives or the owners, and decide they want a comprehensive risk assessment conducted and a program developed. And when we do that, first of all, the actual risk assessment in and of itself is a fairly in-depth project that may take several months. Should they decide they have identified a corporate risk that justifies a program, then we would begin the process of building out a program, which goes much further than just the closed protection operations that would include developing protective intelligence practices, developing security in situations, awareness training programs for the various people who have contact with the executive, travel management, transportation. All those things become a big project that does have a necessary structure in order to ensure certain deadlines are accomplished and goals are met.

0:40:19 S2: It sounds like the risk assessment is a whole project in and of itself, but is it correct to say that the outcome of the risk assessment begins to lay the requirements for what the risk program would do, should a group of owners want to take it on then?

0:40:34 S4: The risk assessment provides them with a road map based on industry best practice and benchmarking, and they then decide based on their risk tolerance, which elements they wanna move forward with. And we sometimes help them with that, to guide them through how to get themselves to a gold standard, for instance. Whereas sometimes, they handle it internally but we are many times the third-party facilitator to analyze the likelihood of incident, look at their vulnerabilities and based, again, on best practice and benchmarking, give them some guidance as to where they should position themselves.

0:41:10 S1: How big is a risk assessment in terms of a pile of requirements? A lot of our PMs might be coming from an IT perspective or other types of development work. Is that a book of thousands of requirements or is that an executive memorandum of a couple key points they're gonna need to pay attention to?

0:41:27 S4: Again, it greatly depends on the organization. So if we're dealing with, for instance, with a pharmaceutical firm, they'll have a variety of risks that they may not have contemplated outside of the standard thought mindset. When you think about bio security, for instance, in many of the scientists' minds, that's the security of the element in the testing process. Whereas in our frame of mind, we're looking at the security of that item as it might pose a risk to insider threat or other biochemical terrorist attacks. So that goes even much more deeper than just looking at site security surveys, and physical security, those programs that have to be evaluated.

0:42:14 S1: How is it that you see those, is that based on the benchmarks or do you have a team that intentionally looks at things from different angles, in that sense? Because I can hear what you're saying is your stakeholders are really focused on the thing that they see as dangerous.

0:42:28 S3: Yeah, so that's a big part of our program is when we do our risk assessments we do a team approach to it because, for instance, my background is very much focused on the behavioral-based threat assessment, whereas I have other people in our team who are scientists with PhDs in microbiology and they can help with that specific type of project. There are other people we reach out to with specific experience in terrorism. So really depending on the footprint, a multinational corporation with many people globally and various perhaps austere environments, we may have to adjust the scope of the risk assessment compared to perhaps just a DC-based firm.

[music]

0:43:17 S1: What would you be looking at when you look at a multinational? Can you frame out the scope somewhat of what you might be having to look at?

0:43:23 S4: First of all, the basics are always to look at crime versus persons, crimes versus property, and understand that. We also do take a look into technological and natural threats that could impact the operation, so while we might automatically as a security professional think that fences and guards and gates are the mitigating strategy, if mother nature is the opponent, that's not gonna do us a lot of good, so we always try to take that holistic approach towards the risk assessment, as well as what the risk could be posed by just geographical positioning close to ISIS or to terrorist organizations. And again, based on the assets they're protecting. Perhaps the assets themselves are of such interest to competitors or to other external parties that we have to evaluate that level of challenge also.

[music]

0:44:23 S1: What constitutes a successful program once it's scoped out? How will you know when you're done?

0:44:28 S4: In the sense of a risk assessment, we're officially done once we've submitted our file report, presented that to the leadership team. They may require us to then engage on pieces or aspects of the project to facilitate mitigating that particular risk, but typically once we delivered it to a leadership team, they've reviewed and accepted those risks and they'll move forward with their security team to address them. If they don't have a security team, many times they rely on us to help make those adjustments.

0:45:01 S1: So let's go on to they've decided they need a risk program, what does a team look like or look at then? Obviously, it's based on the risk assessment that's been accepted and the risk that they think they face, but how do you go about planning for something like that for a multinational?

0:45:16 S4: Well, particularly in a multinational corporation, many times we're gonna find that there are vulnerabilities in the grander scheme of things, perhaps they might be administrative in nature, but we also might encounter physical or operational aspects that have to be addressed also, and in bigger projects we do find project managers embedded into the long-term project. In fact, I have a client right now we're working with that they've assigned a project manager to facilitate understanding the timelines of deliverables and scope of what will be done.

0:45:57 S1: You just hit the exciting button for us.

0:46:00 S4: And I think that this is where your audience perhaps should be excited because the reality is that once risk assessment is done, we've unveiled the underbelly of the client and they have a certain obligation and duty of care to ensure they mitigate the risks that they and their legal counsel, the board of directors, perceive as justifiable. And the flaw in many cases is that we conduct these risk assessments, they sit on somebody's desk, and they fix 5% to 10% because they didn't involve a program or a project manager to come behind them and say, "These are the aspects we can fix, this is the cost to us, these are the long-term costs, and this is the time frame to get to that gold standard."

[music]

0:46:55 S1: From your perspective as someone who's a subject matter expert who's delivered the risk assessment, it's been accepted, it's been worked on, it's understood and now it's time to build the program that mitigates it, that it looks at from close protection to transportation to a general security awareness, probably some, you mentioned behavioral, for example, in your world. Probably some education, more than awareness even, some do's and don'ts and behavioral changes you're expecting, or that they should expect from their organization.

0:47:20 S4: Yeah, there's a lot of things that we find many times that aren't as simple as a door lock's broken. There are many times cultural changes and those types of changes require a bit more effort, such as increasing situational awareness among the company and its employees. That's not just a matter of while we might make a recommendation to a client that that's something they have

to address, the steps to implement that cultural transition require multiple members of a multidisciplinary team to understand between HR and project managers, and legal and security how to make that transition to a more aware culture.

[music]

0:48:08 S1: So, what would it be that you would like to see an organization have from a project management perspective? Here the SME coming in, there's this breadth of parts that need to be changed. What is it that you would need to see from the project manager? You talked about it as a facilitator.

0:48:23 S4: Yeah, I think the biggest thing is that the project manager has to realize that this just isn't a task list. If we add or remove a piece of the recommendations, it can have an impact on the stability of the rest of the program. So, as they're going through and budgeting, perhaps giving guidance to leadership of the firm about moving X piece forward and holding off on Y, that integrated consultation is important to make sure that we understand that if we've taken away the turn signal, but we've increased the headlights, how's that gonna improve the vehicle's performance?

0:49:07 S1: What type of issue would they face where there's an integration problem and they need to be linking what the corporation is expecting to what you're saying needs to be done?

0:49:19 S4: In a broad perspective, this is more on a policy procedure element, but you certainly heard a lot of dialog about insider threat programs. And I imagine that there are many times that that is one of the findings that a project manager might find themselves tasked with facilitating that development of the program. A problem that I encounter many times is that insider threat is collaborative among multiple areas of intelligence. So, if you have a protective intelligence program that protects the executives and their families, you might have a competitive intelligence program that's keeping an eye on those people coming or going that may wanna steal information from the company.

0:50:05 S4: And then, you have your human resources department that has access to the employee assistance program for people with suicidal ideations or domestic violence programs that notify them of individuals that have been targeted by spouses or former spouses for violence. All of that information or intelligence should be collaborated. And if a project manager is given direction by the client that says, "Well, we don't have the funding for protective intelligence right now, so let's just scrap that, focus on the other ones," what you end up with is a void where perhaps the executive assistant or the family of the owners or even the leadership themselves and special event planners may not collect valuable information about people who are approaching or contacting various members of the organization for wrongful purposes. And that same individual, if they reach a road block in trying to reach the executive may find an opportunity with HR to become a contractor or employee.

0:51:22 S1: So, your PM needs to be the integrator, you said, and the facilitator. It's almost like they are the ones making the case for executing against the risks that you've identified that have been accepted as the requirements or as potential problems.

0:51:33 S4: Exactly. And they have to really work with that consultant to understand, "If I do X,

how does that impact Y?"

[music]

0:51:44 S1: So, that puts the PM in a real, from our perspective, a classic position of they're needing to really understand their stakeholders. It seems like that often your stakeholder is different than the people being protected or the people who are representing the information that's being protected or the assets that are being protected. Is that something that the PM would help you facilitate?

0:52:06 S4: Many times, they're just offering a different viewpoint on how to manage that stakeholder relationship. What we find many times, particularly in this larger scale risk assessment, that while most of our contact might be with the chief security officer or legal counsel or human resources, we will still have some contact to the board of directors or leadership team because we don't wanna design a program that isn't fully supported by those stakeholders at the top.

0:52:37 S1: Do you face cases where somebody wants to protect something that somebody else doesn't want to protect?

0:52:43 S4: Absolutely. In fact, the bigger problem is usually turf, in that they all wanna protect it and they all wanna own it. And sometimes we find that a voice of reason needs to be situated somewhere within the organization to say that based on the CSO model produced by ASIS or based on other industry standards, these people should have ownership of these aspects, whether or not you think it's sexy or not. You don't own it. This group will. That's usually where the bigger conflict is for us in stakeholder investment.

0:53:17 S1: And that's where you need your PM to step in and be your facilitator? Or that would be helpful if you have one?

0:53:21 S4: Right, right.

[music]

0:53:27 S1: Let's talk about quality for a second. Presumably, you meet the requirements for the contract and build out the program that they need. How do you know the level of quality that you've provided? Is it just a function of there's no breach, or what are other metrics or measures for that?

0:53:44 S4: Metrics are a very challenging mark point for our industry. Because no news is good news. So I think if we look at metrics more in the sense of how your workplace violence program might be managed, most companies will tell you they don't have a workplace violence; once they establish a program and they actually collect metrics, the first result is since they've turned the lights on, and the skeleton's out of the closet, they find an eruption in incidents that were never reported before. And then, over time, using proper metrics, they can look to see how their educational program, and how their investigative strategies are helping to mitigate the risk and manage those cases that were of most likely presenting danger to the organization. Granted, it still goes back to the threat assessment 101. If nothing happened, then I can only presume that we helped prevent it, but we can't be positive.

[music]

0:55:00 S1: When we're doing risk from a project perspective, which obviously is risk to the effectiveness of a project, not necessarily the risk to something that is being secured, something as dramatic as you may be facing. When we do that we look at the cost of the mitigation, the cost of the potential damage, times probability and things like that. When you help build their budget, do you help look at the potential costs of all of these disruptions and surprises versus the cost of mitigation and prevention?

0:55:32 S4: Yeah, we do. For instance, when we look at a risk assessment for whether or not an organization can justify an executive security program, one of the key things we do is talk to investor relations, and gain an understanding from investor relations, specifically in a publicly-owned company, what the impact would be on shareholder value if X individual had something happen to him. That allows us to put in numbers that the board understands.

[music]

0:56:09 S1: PMs that you end up working with when you have them, are they typically out of the corporate risk management side? Is it the risk managers who are assigned to this or is it usually somebody in security?

0:56:17 S4: It's a mix, actually. I would say 50/50. We have some that are in the risk management department, and others we've encountered that are actually part of the security function.

0:56:26 S1: So, a PM who wanted be in that space, what do they need to know the most of, if they're good PMs that have been trained in some of the basic techniques of project management, making sure that a program is delivered on time, on budget, it's monitored, and things like that, what else do they need to know to be effective in that space? Would they need to come out of a security background?

0:56:43 S4: Not necessarily, no. In fact, I think that the bigger takeaway for them is that as long as they have an open mind and can really take in all the data without some self-imposed, perceived concepts about what Hollywood tells us security's all about, then they probably would function well. There is much, much more that goes into a sophisticated security program that goes beyond that man in the sunglasses.

0:57:13 S1: Ah. So that's why you probably like this guy with the background in complex projects, so he knows how to pull together a lot of parts and operations from a multinational perspective.

0:57:22 S4: Exactly, 'cause when we talk about executive protection, for instance, there are layers of security around the protective function of that principle that that program is dependent upon, and that would fall within some of the shroud or umbrella of a holistic corporate security program, and that corporate security program, depending on how it's aligned within the corporation, will rely upon other aspects to be successful. It's usually more about team work, and cooperation, and understanding there's one goal which is to protect assets, and those assets might be property or people.

[music]

0:58:03 S1: So if it's about team work and cooperation, and making sure things are integrated within the organization, and not to mention budgeting and delivery, it begins to sound a lot like a job for a project manager. Awareness, meticulousness, vigilance, the ability to adjust and readjust the management focal length from big picture to minutiae and back out again is a key skill for this type of work. And note the requirement for skillful stakeholder management. All these elements are crucial to achieving a viable level of security; they also happen to be valued qualities in a project manager. As scary as these times might be, the good news is there are plenty of opportunities and a need for PMs to help. We may not come flying out of a phone booth with a cape and t-shirt emblazoned with PM, but project managers, we can be heroes, we can part of the team.

0:58:52 S1: Special thanks to today's guests Paul Pelletier, Dave Sears, and Chuck Tobin.

0:58:58 S5: Our theme music was composed by Molly Flannery, used with permission. Additional original music by Gary Feldman, Rich Greenblatt, and Lionel Lyles. Closed production performed at Empowered Strategies and technical and web support provided by Potomac Management Resources.

0:59:14 S1: PMPs who have listened to this complete podcast may submit a PDU claim, one PU in the Talent Triangle Strategic and Business Management, with the Project Management Institute's CCR system. Go to CCRS, select Education, and then Online or Digital Medium, and enter provider code C046, the Washington DC Chapter, and the title PMPOV0033 Security.

0:59:37 S1: If any of our listeners have comments about this episode, or past episodes, or ideas for future guests or topics, please go to pmiwdc.org/contact or to our new Facebook page and leave your comments there. You may also contact me directly at kendall.lott@pmiwdc.org, and of course, you can find me on LinkedIn.

0:59:57 S1: I'm your host Kendall Lott and until next time, keep it in scope and get it done.

1:00:03 S5: This podcast is a Final Milestone production, distributed by PMIWDC.