**RedZone Podcast Episode #88: How CIOs Can Use Threat Modelling to Benefit Their Organization: Build Out Your Defenses! With Adam Shostack**

Bill: Right, Adam, have you filled your water glass?

Adam: I have, and I am good to go.

Bill: Fantastic. Well, I want to welcome you to the show today. I'm very excited for our topic of conversation.

Adam: I am, as well. Let's jump in.

Bill: Yeah, let's jump into this. I think ... Did you speak at RSA at one point?

[00:00:30]  
Adam:  
I have spoken at many, many RSAs. I didn't speak this year. I did last. I think I'm on about an every other year rhythm with RSA.

Bill:

[00:01:00] Got it, got it, because I knew it wasn't this year, but I thought possibly I'd stumbled into you the previous year. Then, I'm staring at your book right now, Threat Modeling: Designing for Security. I've been preaching this for years now. I call it security by design, but I've never stumbled into threat modeling.

Before we even jump into threat modeling, why don't you give my listeners a little overview of yourself and then your journey? What led you into the security space? Were you always into security from high school and college or how did this happen for you?

[00:01:30]  
Adam:

[00:02:00]  
I was studying environmental science in college. When you study environmental science, you learn about economics. You learn about these complex, multifaceted problems. I was doing this long enough ago that the jobs of today in solar, in recycling, in energy markets, in pollution markets, all of which I studied ... Those jobs weren't available. I got a job as a Systems Admin at a medical research lab, great laboratory at the Brigham and Women's Hospital in Boston, doing amazing things, bringing patients into an MRI for example and doing surgical procedures inside the MRI machine.

[00:02:30]

[00:03:00]

[00:03:30] Security and privacy was a piece of my job, and I discovered that I enjoyed it. I struck out. I became a consultant. I broke a few things, the way security people do. I broke the secure ID card. I broke the TIS Firewall Toolkit, which, at the time, was the leading open source firewall. From there, I joined a startup building vulnerability scanners. While I was there, we were shipping these scanners. We were saying, how do we think about these vulnerabilities? I met there Steve Christey and Dave Mann, helped them to create the CVE. We sold that startup. I went to another one, went to another, doing patch management. That one didn't go so well, and I said, "You know? I could really use a stable job," and was talking to a number of companies, one of which was Microsoft.

[00:04:00] I said, "I can deal with being at Microsoft for two or three years." A decade later, I decided it was time to move on. It was a fantastic experience for me. I got to work on the Security Development Lifecycle Team, where I did work on threat modeling. Excuse me. I got to do some analysis of how computers get broken into. That led to pushing the fix for autorun out through the Windows Update Channel, prevented a lot of infections through VAS, and then I said, "I'm going to go build another startup. That one didn't work the way I hoped it would.

[00:04:30]

[00:05:00] As I was working the phones, saying, "Hey, can I interest you in these things that I'm building," people were calling me up and saying, "Hey, Adam, can you help us threat model? Can you help us do security engineering?" That's where I am today, working independently with a variety of organizations. That's the strange, meandering path. If you'd asked me to predict any of that, I couldn't have done it.

Bill:

[00:05:30] Well, what's really interesting is your book, Threat Modeling, which I really enjoyed reading. I've listened to you online and through YouTube, and just trying to understand a little bit about what threat modeling is. Let's start out there. What is threat modeling? Then, we have to talk about why, because I think a lot of my listeners, when they think of threat modeling, it could be seen as, "Ugh! Something else I have to do with security," but I want to really hit it hard upfront, the value, what threat modeling brings to bear. For all listeners, we're going to cover GDPR. We're going to cover privacy. We're going to cover getting a seat at the table. I mean, we're going to bring it with security today, but I want to start out with your expertise with threat modeling and why, and what is that?

[00:06:00]  
Adam:

[00:06:30]  
Okay, so let me be concrete to start out, because when you deal with models, it gets very abstract very quickly. Threat modeling is a set of ways to answer four key questions about anything you're working on. The first question is what are we working on? Developing that common understanding between security experts, between architects, between operations people. Here's a picture that we can all point to of what it is that we are building, what it is we are deploying, what it is we're selling. Question one: What are we working on? Question two: What can go wrong?

[00:07:00]

[00:07:30] There's a number of ways you answer that. You can think about ... There's a mnemonic, STRIDE, common threats of spoofing, tampering, repudiation, info disclosure, others. You can use a kill chain to think about what can go wrong. You can brain storm to think about what can go wrong. And then what are we gonna do about it? How are we going to address these issues that we're finding, and did we do a good job? And so that's the essence of all threat modeling techniques. You can get super deep and waterfall. You can build these formal diagrams, you can create these long lists of threats, and you can be very agile. You can stand at a whiteboard and produce post-it notes that say, "We're going to address this spoofing issue right here," and write that on a post-it note, stick it on your Kanban board.

[00:08:00] All of these are ways to get security into a conversation about how we can build better products, better services, whatever it is we're building, we want to bring security in these days. And so threat modeling is the collection of techniques that lets us do that.

Bill:  
[00:08:30]

[00:09:00] That makes sense. So it's a collection of techniques that allows you to address ... Would you be able to put a problem set through this lens? As you're working with an organization and trying to help their teams get better at this, would they approach a system with threat modeling with these four questions, for example, an E-commerce system as a whole, or a problem set like how does GDPR impact us? Where would you start with threat modeling? Is it super tactical, or do you apply it through kind of a bigger picture strategic lens.

Adam:

[00:09:30]

[00:10:00]

[00:10:30] Yes. You can go either way. And this is one of the things that makes threat modeling a little intimidating for people, is let's say your organization is working on a GDPR process right now. Better move quickly, and we can look, what are all ... And you have to do this for GDPR. What are all the data flows that we have? Where does data go? Who can see it? We can work with that, or we can work with, we're deploying an E-commerce application. Great. Are we deploying V1, or are we deploying V6? Maybe V6 has ... We're adding a IOT payment API. Okay, let's start by looking right at that new API. Let's get very, very focused, let's get tactical, and say "What can go wrong with this API," because that's the scope of the project that the team is working right now. If you go to them and say, "Hey, you're building out the V7 API for IOT payments, but really what I need you to do is this whole GDPR project," well, that's great, Adam. Thank you so much for your input, and we'll be in touch about that. You've got to work with what a team is ready to work with, and you can threat model as part of either of those projects.

Bill: Well, Adam, you know, as we move through our conversation, what struck me with your book is that we talked about what's your threat model, then you have this really important smart technique that you developed called, STRIDE.

[00:00:30] Before we get into what STRIDE is, I want you to explain what STRIDE is in a few moments. One of the things I think a CFO has an advantage of and even a building engineer has an advantage right now, is that we've been putting buildings up for a 100 years and we've been accounting for systems financially for maybe since Mesopotamia or since, at least the Egyptian pyramids.

We've had a long track record and there's structure in a format to debits and credits, and to general ledger, and to income statements, balance sheets, it's just a very structured rigorous process that we have lots of people trained on.

[00:01:00] Unless you are ethically challenged or morally challenged, a CFO can be reasonably assured that the data is going in correctly when they're looking at the financial summary of a business. Similarly with putting up a complex building, that we have engineers and disciplines across all sorts of trades and multiple companies and subcontractors, participating and putting up safe buildings.

[00:01:30] One of the things I wanted to talk to you about is STRIDE essentially what you would say possibly like a structured or systematic way to analyze a complex system and layer in security into it?

Adam:

[00:02:00] Absolutely. It's a way to help you see what problems are going to happen. Even before you get to layering security on, making trade offs about what you're going to do, when things are still fluid. I like your building example. Once you've poured the foundation, the size of the building is pretty much set. Once you start laying the code, the structure of that code gets more and more set. STRIDE was invented at Microsoft as a way of bringing some structure and consistency, and actually predates my time there.

[00:02:30]

[00:03:00] Let me talk about what STRIDE is. It's a [inaudible 00:02:31] for the most common threats that software faces. There's spoofing is the S and an example of this, there was an article this weekend about a payments transfer system and what people would do is, give you a phone number and say, hey, make the payment to this phone number, and I thought I was talking to you to pay for the beers we might have had last night. But it's really someone else, but I put in that phone number, the payment went to them. There was a confusion about identity, about authenticity and now my money is gone.

[00:03:30]

[00:04:00] The T stands for tampering. We saw an example of this in Washington D.C. recently, where some cabinet secretary edited the emails that he was sending to his ethics officer before getting permission to bring his wife on a trip. He tampered with that email. There's reputation, saying, I'm sorry, I didn't get the calendar invite, would have loved to join that meeting, hm, hm, hm. There's information disclosure. This is like what's happened with Cambridge Analytica and Facebook. Information was collected in ways that people didn't expect, didn't understand. They were very upset.

The D, denial of service for ... My favorite example of this is all the video cameras in the world got turned into a bot nest, took a DNS provider offline and knocked a good chunk of the Internet offline by flooding that DNS provider.

[00:04:30] And then, E stands for elevation of privilege. A good example of an elevation of privileged hack, might be, oh, I just had one here.

Bill: Well, I mean, in the elevation of privilege is, that's sorta like a Holy Grail. I mean, that's what the advance persistent threats were hitting five years ago. Not that they're not now, but that's going laterally behind the firewall is certainly one of the pieces that you're referring to in that analogy, right?

[00:05:00]  
Adam:  
Absolutely. Just to recap, STRIDE stands for spoofing, tampering, repudiation, info disclosure, denial of service, and elevation of privilege. It is a way to structure your approach to make sure that as you look at a system, you will find a breadth of threats rather than getting trapped in one little area in your analysis.

[00:05:30]  
Bill:  
That makes sense. Now, when you were working with ... With STRIDE, one of the things that you were talking about was different traps that you see through your work. I think this is interesting for people to think, what can go wrong, like, what are some of the traps that you see security teams, architects, socios fall into.

[00:06:00] Again, you don't have to go through all seven, I think you have seven or ten, but maybe just a couple that you find are the top ones, that may be related to those that are trying to tackle Cloud, security, right now, or they're trying to tackle a GDPR and privacy, or it could be a complex system design, whatever it may be, what do you think of the top one or two traps that architects are falling into or citizens are falling into now?

[00:06:30]  
Adam:  
The first trap is to look at threat modeling as a monolith that there's a way to threat model in the same way that we have lots of programming languages, programming paradigms, programming tools, we have lots of ways to threat model, we have languages, we have tools that you can use, and you can plug and play them.

[00:07:00] If you want a threat model agilely, you're going to do it differently than if you're doing it at a waterfall. If you want a threat model IOT, you're going to do that differently than if you're threat modeling a Cloud service. In the same way that it's all software development, it's all threat modeling. The first trap is that monolithic perspective of the way to do it is versus the ways to do it are.

[00:07:30] The second trap that I think is worth calling out is, thinking that this will be easy the first time you do it. To continue the programming metaphor, we start writing code with a hello world sort of program. If you want to start by threat modeling, a car, a nation state attack, that can involve a lot of moving parts. It can be difficult.

[00:08:00] Realizing that you need to start small, start with what you're working on right now, develop those skills and over time you'll get better and better at it. Versus, thinking, hey, this will be a cake walk the first time out. I don't want to discourage anyone.

The same way that the first time you might use Git. It's challenging to use Git and then once you've gotten over that hump, it turns out to be a really interesting paradigm shift. It changes the way we develop software and that refers to both Git and threat modeling. I'd say those are the top two traps.

[00:08:30]  
Bill:  
I think also, what's really interesting, and I know you and I share this and we cover this in the book, The Checklist Manifesto. What's so impressive about your work that you put together in this book is, the multiple ways that I think, this back to your agile piece, which you and I talk about, and it talked about extensively, is how we can enable security to go fast.

[00:09:00] I love this kind of modularity that you have with threat modeling that you can take these checklists that you've developed in your book. I think they can be used as a large, like you said, waterfall type checklist or they can just checklist a rapid iteration around a threat model of a certain scenario or a certain system. I think that's impressive, what you put together here.

Adam: Well, thank you. Yeah. Thank you.

Bill:

[00:20:00]  
So one of the things that I wanted to ask you about related to your approach with threat modeling is, how does it differ, or how is it similar to some of the government style oriented check-the-box compliance programs like PCI ... Or, that's not really government. But like GDPR, NIST, or ISO, or these frameworks. I love using this word framework, 'cause everybody's using it these days. But what is the difference between your approach with threat modeling and some of these other kind of standards that are out there?

[00:20:30]  
Adam:  
So that's an interesting question, and I'm trying to decide ... Let me focus in on two aspects of it.

Bill:

[00:21:00] Or, you know what, before you ... I'm gonna give you some more time to think about it, 'cause that's a packed question. One of the problems I have with the government standards is they don't tell you how to fix things, and they don't tell you if your systems are any good, they don't tell you if you have overlapping functionality between systems, they don't tell you how to budget, none of that. They just say it's good or bad, and by the way here's your general high risk areas and your medium ... But they don't tell you how to fix it, and that's a problem that I have with this. And not being an expert in threat modeling, I'm just wondering where you would slot in if you were asked that question.

Adam:  
[00:21:30] So the first thing I would say is threat modeling is simple. If you and i were to threat model my house, and we've never met in person, you've never been here. But if I were to ask you to threat model ... Let me actually do this. If you were to break into my house, how would you start?

Bill:

[00:22:00] Wow, that's a great question. I would look and see what sort of defenses you have in your first floor versus your second floor, if you even had a second floor. I would have to ascertain whether you had motion sensors. I'd have to see whether ... I would look at the locks, and I'd have to examine back entry ways.

Adam:

[00:22:30]

[00:23:00]

[00:23:30] So you get it, right? This isn't that hard to do, and a lot of these government standards, and in fact a lot of the threat modeling processes out there layer in a lot of complexity. The simple question that any decision maker can answer is what are we working on here? If you can't answer that, there's a bigger problem going on. But they know how to answer that, and then a system like STRIDE gives them a way to walk through the doors, the windows, the first floors, the second floors, and analyze them. And one of the things when you make a government standard, when you make something like PCI, you're trying to pack in all of the things that might go wrong with any system. And so you end up with these very long lists of this might go wrong, that might go wrong. I'll use PCI as an example. I don't really want to pick on them, but one of the elements of PCI the last time I looked at it was make sure the seeds for your cryptographic random number generators are strong. And that was an item at about the same level as make sure you use anti-malware software. Now, I don't know about the attackers that you deal with in your business, but the ones I deal with tend to start from the simple, and they're not gonna reverse engineer your random number generator in most circumstances.

[00:24:00]  
Bill:  
Or put your anti-malware in between all of the encrypted systems that are all of a sudden supposed to show up on your network.

Adam:  
[00:24:30]

[00:25:00] Yeah. And so these standards end up containing mitigations for threats where the likelihood may be low, there are easier paths in, but you've got to deal with that, and you're going to be dinged the same number of points in your audit, in your assessment, because you're missing line 16 or you're missing line 17. The reason I like to start with threat modeling is because it gives the strategic overview of what you're working on now. And so, rather than saying, "Hey, here's a thing you must do," why don't we start from what you are doing, and make sure we develop the right security measures to control it?

Bill: When you say what we are working on now, what do you mean by that, when you say that sentence? What are we working on now?

[00:25:30]  
Adam:

[00:26:00]

[00:26:30]  
So I have used that same sentence to refer to thing in scale, like of Windows 7 or Xbox Live, and a training course I did for a customer recently, we started from a one sentence description of, "You're working on a mobile phone app to transfer money between customers." You can take that single sentence and develop a threat model from it, or you can take a system like Xbox Live, and develop and answer to, "What is this system as a whole?" And so I really do mean, what are we working on? How do we develop common models of that system so that we can have an engineering conversation about what this system is? And a lot of the systems I work on are so large that no one has an understanding of the system as a whole anymore, and one of the reasons that that's challenging is because everyone brings a slightly different mental model of what's going on.

[00:27:00]

[00:27:30]

[00:28:00] Let's say we were threat modeling Gmail. Maybe I believe that looking up the blacklists for anti-spam is your responsibility, and you believe it's my responsibility. And so it falls through a gap, because we don't have a common model. And so when you ask what do I mean by what are we working on, it's really a very, very ... And I hate to be buzzwordy, it's a multiscalar question. The question expands and contracts to the sort of answer that the person, the team, the department, the organization is answering. And it's a starting point question, 'cause once we start building that model of what it is we're working on, it allows us to say, "Yeah, here's the thing for this next release. This piece here's out of scope." Super important to be able to say this is out of scope.

[00:28:30] You don't want to boil the ocean, and you certainly don't want to be looking at a big complex system the first time you threat model, and saying, "Wow, we found all these really exciting threats to this code that was written 15 years ago, and now we have to do something about it." Now maybe, big project, you'll discover that if you find a big problem, you go to management, you say, "Hey, we need some time to fix this," you'll get that time, 'cause you discovered a big problem. You don't just want to sit on it. But if you don't scope, if you don't know here's what we think we can work on right now, it ends up being mushy. Does that help? Does that give you a context for how I'm using the question?

[00:29:00]  
Bill:

[00:29:30]  
For sure, and I think it's a lens of clarity, and it's a lens of focus. And I want to also indirectly and directly answer the question, "Why threat model?" And I think one of the questions I'm asked quite frequently is, when top decision makers, the CIO, the CISO are wanting to move into the cloud, and there's a stretch, there's this hybrid stretch that happens between the data center or centers and the assets that are in the cloud. And the question then would be, to get clarity ... Let me ask you this, what would be a good question to ask that would then prompt a good threat modeling exercise? Like how do I security my cloud resources? What would you say the good question would be?

Adam:  
[00:30:00]

[00:30:30] So one of the challenges that people encounter as they move to the cloud is they have a set of defenses that they've come to rely upon in the data center world, in the desktop world. And as you move to the cloud, often times there's two changes that are happening. One is we're giving up control of the hardware, and two is we're moving in some fashion from a waterfall to an SRA, to a CICG, to a dev op sort of model, and the question becomes, what's the security difference between where we were and where we're going?

[00:31:00]

[00:31:30]

[00:32:00] And I find the way that threat modeling really helps people is to start in the middle and say, what are we gonna do about it? We have a set of controls of our firewalls. We have a set of control anti- malware. We have a set of controls multifactor off. Why do we have these controls? What is the strategic goal of the firewall? It's isolation. What's the goal of the anti-malware? It's prevention and response around the integrity of the code running on that system. How do we achieve those same goal in the cloud? Do we need the same sorts of isolation on a network segment by network segment basis, or do we want to isolate on a machine by machine basis because we know that we're in someone else's data center, and so our tools transform. What are we gonna do about it? We had a set of answers when we were in our own data center. The questions about what can go wrong, the answers don't change that much. What are we gonna do about it can look very, very different.

[00:32:30]

[00:33:00] And the people I've seen succeed in moving to the cloud are not trying to do a one for one replication of, "These are our controls in the data center, therefore they will be our controls in the cloud." What they're doing is they're modeling, they're saying we have this control for this reason. How do we address that reason in a cloud native way, in a hybrid native way, rather than we're gonna shove all of this stuff that we've accumulated over the years. I'll tell you, the people who are doing that well are discovering a lightness and an agility where a small number of controls turn out to replace a large number of control that have accumulated over 15 and 20 years in the data center, and they don't necessarily need all of them as they move into the cloud.

Bill: Yeah, that's interesting. So that lightness and agility is needed when the business needs to go quicker and faster. We don't want to lose the governance and the security, but what you're saying is you're finding people are kind of cleaning out the closets a bit, and still putting the controls in the cloud, but with an increased agility and speed, potentially.

[00:33:30]  
Adam:

[00:34:00]

[00:34:30]  
Yes. And I'll give you an example. I was talking to someone about the question of how we upgrade our database servers, 'cause they have started the process of learning to automate their builds. And they said, "Okay, so the web front ends. We automate those builds, it's great, we have a consistent way to do it, we can apply a patch, we can roll out a new version to all our front ends. What do we do to patch our database servers?" Seems like a reasonable question, right? We need to maintain ... We can't just roll out a new database server, because we lose all the data. And the question that I turned around and asked them is why are you operating database servers at all? All of the cloud providers will give you data storage as a service. They will patch those machines, they will manage those machines, and your interface to it is now the data reads, data writes, in whatever form works for you, and you can give up on managing database servers. Isn't that easier? Focus in on your core business.

[00:35:00]  
Bill:  
And then, did that prompt another series of questions to ask how would that new paradigm work of securing the database from ... For example, that paradigm essentially from a patching perspective makes sense, but what about the encrypting at the file level versus the record level? Did it prompt a whole other series of questions about securing it?

Adam: It did, and the other question frankly that it prompted is, are we getting locked in?

Bill: Okay.

[00:35:30]  
Adam:  
And you know, the big cloud providers these days have encryption options that they will manage for you. You can set things with an API to say, "I need this data to be encrypted at rest." It's hard, frankly, with these systems to get the data in motion to be unencrypted over the wire, you have to work at that.

Bill: Sure.

[00:36:00]  
Adam:

[00:36:30]  
And so instead of, "We're gonna deploy this control," we're going to call this API as part of initialization. We're gonna call this other API on a daily basis to make sure it comes back and tells us our data is still encrypted, and it becomes an SRA task to ensure that the control is operational on an ongoing basis. And it's a lightening of the load, it's an automation of the load that's a really interesting transform as we move to the cloud.

Bill:

[00:37:00] Interesting. Yeah, I like that quite a bit. Well, I liked how we kind of telescoped there. As we wrap up, Adam, I wanted to talk about having a seat at the table and how we can get ... So I think the big question is why threat model? And does it give us the ability to communicate more powerfully, higher up the chain, up to the board, to the senior exec level? And what has been your experience with that, with threat modeling?

Adam:  
[00:37:30]

[00:38:00] Well, that's a great question, and there's a lot. So let me start at the question the board wants to ask, which is are we building our products, are we delivering our services with security in mind? And historically the answer to that question has been no, and the reason it's been no is because security shows up at the end and says, "Here's your pen test report. Here's your list of vulnerabilities." We haven't necessarily had the tools, the deliverables, the forms that people look for. They look at security and say, " If you want to sit at the table, what are you gonna do when you're there? How is this going to be consistent, rather than ask two experts, get three answers?" Those behaviors, that lack of structure made it hard for security to engage in design conversations.

[00:38:30]

[00:39:00]

[00:39:30] Threat modeling gives us a way to get structured, to have consistency between the experts, so that when the boards says, "Is security part of our engineering process?" the answer is yes. It's not a bolt on, it's not an audit at the end. It's what are we working on here together, what can go wrong? And these are questions that engineers ask. What can go wrong with reliability? What can go wrong with scalability? What can go wrong with our cloud transition? What are we gonna do about it? And by structuring things in this way, security gets to be a full partner in the organization's transformations, these digital transformations, these cloud transformations. Marc Andreessen, the venture capitalist, says software's eating the world, and Fraser Scott says, "Hackers are eating your software." Which I think is just a great high-level, this is why we need to do this. Threat modeling lets us prevent comprehensively, systematically, in a structured way, in a predictable way, those hackers from eating your software. And it's all about getting started.

[00:40:00]  
Bill:

[00:40:30]  
Well, I do think that GDPR is gonna force that conversation into building privacy by design. I myself have seen it now many times where if we just layer in security right at the front or at least pre-beta for the apps that are being rolled out now, we catch so many design issues out of the gate, it's less expensive to build security in upfront, and it allows the business to go faster than to all of a sudden like, "We forgot we didn't ever ask these questions upfront." So I like that threat modeling is a rigorous way of measuring twice, cut once.

Adam:  
[00:41:00] Absolutely. And let me actually push way back on the pre-beta. You can threat model before you've written a line of code. You can do it agilely, and when you get in there before ... There's no cheaper time to fix a design issue than before it's been committed to Git.

Bill: Ah okay, I see what you're saying. So you can do it on just sticky notes on a whiteboard.

Adam: Absolutely. Absolutely. And it is so powerful as a business transformation to let the business go faster with more confidence, to start on day one.

[00:41:30]  
Bill:  
Yeah, and I think-

Adam: Rather than starting at the beta.

Bill:

[00:42:00] And that's what boards, I think, want to hear, is not that defense is getting in the way of revenue generation. And I think when folks are listening here looking at threat modeling, these are tools, this is a technique to ... Imagining what you're gonna say to the board when you finally have that seat at the table is not that the business needs to go slow, but these are tools that enable the business to have much more confidence and assurity with design, with architecture, so that customers are safe and secure, and that there's a strong value proposition there, but it's not that defense is gonna get in the way. It's an enabler.

Adam:

[00:42:30]

[00:43:00] Absolutely. And let me add one more bit of that value proposition which you expressed so well. The regulatory compliance, and I know we all hate the word compliance, but GDPR is just about here. You don't have a choice. They're looking for evidence that you thought about privacy and security early. I saw something last week at RSA from the Food and Drug Administration. They're looking to see security before you build, as you build. We're gonna see that in more and more industries. We're gonna see that both horizontally and vertically. The Federal Trade Commission talks about building security in. And so threat modeling is a way to structure and accelerate and reduce cost, around all of these security activities.

Bill:

[00:43:30] Well, Adam, I really appreciate you for coming on. This has been a really powerful conversation, well timed for what's happening today. But this is a conversation I want people to be able to know they can reach out, certainly buy your book "Threat Modeling," by Adam Shostack. Did I pronounce your last name correctly?

Adam: I usually say Shostack, but life's too short.

Bill: Shostack. Adam Shostack. But what about if people want to just engage, kind of reach out to you personally? What would you recommend? Through your website, through Linkedin, what is your preference?

Adam:  
[00:44:00]

[00:44:30] My preference is what works for your listeners. I'm on Linkedin, I have a little business site at Associates.Shostack.org, S-H- O-S-T-A-C-K, dot org. And I love doing this. I find real joy in teaching organizations to fish. F-I-S-H, not P-H-I-S-H. I enjoy teaching people to fish in the email sense too. It gives them a sense of how these attacks work. But really helping organizations feed themselves and stand on their own feet with this security thing that's coming down the pike that they need to do, I really have been enjoying the heck out of it.

Bill:

[00:45:00] Well, I hope this has been helpful, and I'm sure it has, for all of my listeners, and I'm glad that we got a chance to share your expertise, because this is quite a program, it's quite a methodology that you have developed through your book and sharing your expertise with the world. So i appreciate that, and I encourage listeners to reach out to you as they need to find ninjas who can just rip the complexity out of environments and help people pave a pathway of a secure yet agile future. So thank you very much, Adam.

Adam: Thank you, it was a pleasure.