When it Mattered

Episode 5: Aaron Warner

Chitra: Hello and welcome to When it Mattered. I'm your host, Chitra Ragavan. I'm also the founder and CEO of Goodstory Consulting, an advisory firm helping technology startups find their narrative.

Chitra: On this weekly podcast, we invite leaders from around the world to share one personal story that changed the course of their life and work and how they lead and deal with adversity.

Chitra: Through these stories, we take you behind the scenes to get an inside perspective of some of the most eventful moments of our time.

Chitra: On this episode we will be talking to Aaron Warner, the Founder and CEO of ProCircular. The Iowa-based cyber security firm helps companies confidently manage their cybersecurity risks. Aaron started ProCircular after a 22-year background as a CIO and CTO in the biotech world.

Chitra: Aaron, welcome to the podcast.

Aaron: Thank you, Chitra.

Chitra: You have a really fun job. Basically, companies pay you to hack into their systems so that you can show them the holes in their security fabric and then you help patch up those holes. It's a bit of an edgy counterculture type of job. How did you get into it?

Aaron: That's a good question, Chitra. I actually come from a very academic family. There are a number of different people in our family that have PhDs and this, that and the other thing.

Aaron: My grandfather actually was one of the people who was involved in creating standardized testing at the University of Iowa, so the work that they did led to things like the SAT and the ACT.

Aaron: I actually went sort of a different direction. I spent a lot of time as a kid on my Commodore 64. I never really went the academic direction. In fact,

the fact that I don't have my doctorate, my grandfather sort of went to his grave disappointed about.

Aaron: I was always interested in computing. I'm always interested in music. Ended up in high school playing in a metal band, actually. Found ourselves as the sort of house band for a biker bar before bikers were all lawyers and hedge fund managers. It led to some really interesting situations. I learned a lot from some of those experiences.

Chitra: Tell us about, what was your band called, first of all, and what were some of the experiences you had, and what convinced you to create a metal band of all things?

Aaron: The naming of the band actually was one of the things that I've carried into business world and that's a really bad name, if you don't think it through, can follow you for the rest of your career.

Aaron: So our band was called Noise Ordinance. The group actually went a variety of different directions. My guitar player's now the president at a global biotech firm, drummer is a professor of optometry, other guitar player works for a fairly large food organization on the East Coast, and our bass player went on to the Marines and then ended up working in the defense intelligence world. So they're pretty nontraditional approach, our band.

Aaron: So Noise Ordinance, we were this house band at a bar in a very small town in Riverside, Iowa, called the Iron Horse. The first night that we played, I was 16 years old. I don't know what my parents were thinking, letting me go to this bar in the first place, but somehow we talked them into it.

Aaron: We got together and thought, "What's our target audience? What's the group that we're really trying to speak to?" Did a little bit of homework and discovered that the bikers all sort of held out a Born To Be Wild. That was a song that we were going to knock out of the park.

Aaron: I will, to this day, never forget the last four chords of that song. When we finished, the crowd was silent. The bikers were very clearly angry with us, and some of them were sort of reaching to their bottle upside down so that they could throw these things at us. They were looking at us trying to figure out whether they could physically throw us out of the bar.

Aaron: And then I looked over to the guitar player and said, "You know, we're going to die. We're in physical risk right now."

Chitra: Why were they angry with you?

Aaron: Well, as it turns out, that song, especially with bikers in the '70s, is something of an anthem, and we didn't realize this at the time, but for a bunch of 16-year-old kids to get up and play their song and try and take it on as their own, none of us even own motorcycles, so it was sort of treading on their territory and they made it abundantly clear that we'd crossed the line.

Aaron: But I guess the lesson learned, if you have failed in front of a bunch of bikers like that, if you're in physical risk for your life, any boardroom that you walk into, any meeting with a customer or meeting with a lawyer, and none of those things look nearly as scary as they might otherwise, I mean, the chances that you're going to leave a conference room alive, the chances that somebody in a deposition is going to throw a bottle at you are actually very low.

Aaron: So, relative to that, everything else looks pretty straightforward, and honestly, that's been one of the lessons that I've kind of carried forward into the work that I do today.

Chitra: Well, when you first entered the workforce, did you actually think about that moment when you had to go into a difficult situation?

Aaron: Yeah. You sort of refer back to that at every turn and you think it could be bad. You could fail at this. But it's probably not going to be that bad and it's probably not like a life-threatening situation. So it's certainly something that comes up over and over again.

Aaron: And actually, the other members of the band bring that up quite a bit. They have presentations to their board, or they have investors that they have to work with, or they have to defend a research paper that they've written. It's never quite as bad as failing at Born To Be Wild in front of a bunch of bikers.

Chitra: How did you get out of there alive? What appeased them?

Aaron: Yeah, the bar was the Iron Horse Saloon in Riverside, Iowa. It no longer exists. I think, thankfully, the place was condemned.

Aaron: We got out of there by focusing on the next song and playing as well as we could, and by the end of the night we had turned that crowd around and they asked us to come back and play, and we actually played the last night that the bar was open. So it worked out pretty well for everyone in the long run.

Chitra: I'm assuming you didn't play the same song on that last night, or did you?

Aaron: I don't believe that was on the set list, no. It was still not our song.

Chitra: So that experience of sticking with something in a difficult situation also probably had a lot of inspiration for you down the line.

Aaron: Yeah. It's easy to say, but in practice it's much more difficult. When things get difficult, when things don't go the direction that you thought they might or that you hope they would, that, I think, is what sort of separates the wheat from the chaff.

Aaron: Just in my experience, that's where you learn the most. That's the place where those big parts of who you are really are defined. Am I going to put my head down and work through this, or am I going to throw up my hands? And I just have never been one to throw up my hands and walk away.

Chitra: Do you think the bikers didn't throw bottles at you because they saw you sticking it out?

Aaron: I think they respected what we were doing, because it took about three seconds for us to get into the next song, and they thought, "Well, these kids have sort of stuck with it. Maybe we're going to give them a chance."

Aaron: By the end of the night we had a whole bunch of new friends, none of which my parents probably would have approved of.

Chitra: So how did you get from there into the cybersecurity world?

Aaron: Well, I had always done computer work. It was always something that I'd put my time into. I didn't know any better. I just thought that that's what other people did with their free time.

Aaron: And it was actually through the band. I met the bass player in another band. He was actually about to defend his dissertation at University of Iowa in computer science.

Aaron: Iowa City is like that. Everybody's involved with the university in some way or another. He said, "I've got to defend my dissertation. I've been putting this off and I have this company, this little biotech company in Coralville, Iowa, just outside of town, and they need some software

written, they need a network installed, and I know that you could do it." And I said, "I'll take a look."

Aaron: So I went out, met with this little biotech company, a guy by the name of Joe Walder 00:08:59. The company was called Integrated DNA and I did some work for them. They were happy with it and Joe said to me, "Aaron, we'd really like you to join the company."

Aaron: At the time I was 20. I said, "No, I have dropped out of school twice now to take on computer-related projects and I can't do that. My family is going to kill me if I don't at least get my master's degree." And Joe said, "Well, we'll pay for that, if you'd like. We'd really like you to join the company."

Aaron: So, I hadn't really thought of that angle, and fast forward 22 years, I was the CIO of a global biotech firm, and cybersecurity was a really major part of what we did as an organization to protect intellectual property and that sort of thing.

Aaron: Truth be told, cybersecurity, and it really wasn't called that in the late '80s, but I had always been involved in sort of the hacking community and trying to test other systems. Friends and I used to email each other's administrative passwords back to one another, but back before you used a mouse to do that, and it translated really well into the work that we did at at IDT.

Chitra: So what are some of the trends that you're seeing in the cybersecurity space now, in terms of the threats that you are confronting for these companies and helping them manage their risk?

Aaron: You know, it's interesting. We started the firm in 2016 just before the election, so we've been involved in some election security work, we have worked with a couple of different companies, a couple of different municipalities that are on the receiving end of some of the attacks that are coming from overseas, so we've definitely seen an uptick. In fact, because we have been involved just by proxy, we've seen an increase in the attacks on our organizatfrom overseas, and it's primarily from Russia or from organizations affiliated with the Russian Government. Other trends that we see, ransomware and you see these cities being locked up and held for ransom for X thousand dollars in bitcoin, tat has happened over and over and over again. I guess the other thing that we see, probably taking a step back over the years, the biggest change, in the late '80s, early '90s, it really wasn't about financial fraud. The internet didn't look then like it does today. The people were who were in that world, who were in the hacking world, were mostly curious, were just

technical people who it was a lot like solving a problem or putting together a puzzle to get into somebody's computer system. Very rarely would you run into somebody who would get in there and destroy things or hold somebody for ransom or steal money with it. It just wasn't part of the scene. And over the years, I think that's probably one of the biggest changes, is that it's become about financial fraud and theft. It's become so much easier to do that to other people. Because of the internet, the threat, it used to be that only kids who had computers, either in the library or, in my case, in the back of the physics lab, weren't able to even get on the internet, and now everyone in Nigeria has a phone that you can use to get on the internet. So, just the sheer number of people who can get connected and who can use those methods, those tools that have evolved over time I think has driven that major change and how fraud and the internet is used against people

Chitra: And there aren't really a lot of easy answers when it comes to, say, ransomware and how you deal with things like that.

Aaron: I actually was joking with a friend. I recently had a conversation with about 10 other cybersecurity professionals and I think there were about 11 different opinions on the subject. It is really not cut and dry. You take the example of the City of Atlanta. I believe that the attack went down over the weekend, so that hacking group had been in Atlanta's computer system for quite a while, but they got notification of the ransomware on a Saturday or a Sunday, and the mayor made a conscious effort not to pay the ransom. I believe at the time the ransom was something like $52,000. Then you get to Monday and CNN shows up, and the FBI shows up, and all of the rest of the press show up, and if that mayor had done his homework, he would have found that the group that was holding them ransom was actually pretty good about giving keys back. So I don't know that the term "good thief" applies there, but they were definitely not the shadiest of those groups. And the problem is that once CNN has shown up, you couldn't give them $52 million. At that point the hackers are just interested in getting out and not getting caught. So it's going to take them years to restore those data. Had they paid that $52,000 I think they would be light years ahead of where they are now. I think that it's a situational question: overall, what is the relative risk? And that's sort of a theme in the world of cybersecurity and in my life, looking at the risk and looking at, right, so what are the benefits? What's the likelihood versus the impact? What's the potential outcomes. If you, Chitra, were to have your computer held by ransom, but you had good backups and you knew, "I can get most of this stuff back, maybe I lose a day." You can tell that hacker to go kick rocks, and it actually feels really great to do that. But at the same time, if they have every picture that you've taken of your family and you don't have it backed up, maybe paying that $300 or at

least just taking the chance, maybe it's worth it to you. So I don't think it's as black and white as, you know, we don't negotiate with terrorists. I really don't see it in that light.

Aaron: Up until recently, the official FBI guidance was that if it's under $100,000, they recommended that maybe you consider paying. It was sort of unofficial guidance that you would hear. I think they've since changed their tune a bit, but yeah, it's a pretty interesting situation. Cybersecurity is a little bit like the Wild West in that respect.

Chitra: and when you educate your potential clients or clients about it, what are some of the ways in which you do that? You probably have some really cool stories or devices or pieces of technology that you use to show just how easy hacking can be.

Aaron: All of us here are pretty passionate about about this work. We like to collect the things that cause problems.

Aaron: A lot of the folks in the white hat world really love to solve puzzles, to solve problems. We actually have a team, I think, that's going down to DEF CON, the big hacker conference, to compete in the car hacking competition that they have.

Aaron: I think one of the big auto manufacturers has put a truck up, so some members of our team are going to go down and try and take down the truck and see if they can get it to lock up and start the car and hit the brakes and all kinds of scary things that you hear online as cars become more and more computer systems with wheels.

Aaron: So that's just one example of some of the things that we do here to stay current, to stay on top of what are the real risks out there?

Chitra: And as the field is constantly evolving, and it's a highly competitive field and cyber engineers, cybersecurity engineers are a different generation and speak a different language probably than you do, even though you're very sophisticated and you've been doing this since you were a young kid, is there a generational divide, and if yes, how do you deal with it?

Aaron: I don't know if there's a generational divide. I think the methods, the priorities that people have maybe is different, but the thing that we all share is a passion for this world. I think the people here feel a really strong sense of wanting to protect people or wanting to help others. All of us really love to solve problems, especially the more complex the better.

Aaron: John McAfee actually had an interesting quote. He said, "If the FBI would hire people with blue Mohawks, they wouldn't have had to outsource the cracking of the iPhone."

Aaron: So, you kind of keep an environment where people are free to be themselves, where people are free to keep it interesting. We have engineers show up here all the time with different tools and devices, and as long as you're cool with an environment where people get to be themselves, I think you get a reputation for being a place that people want to work, and that really gives you access to the best and brightest in the industry.

Aaron: If you try and nail them down and make them be that person that fits into your corporate culture, God forbid try and make them wear a tie, I think you'll find yourself really challenged placing cybersecurity engineers. The demand is so high that those folks can work pretty much wherever they want.

Chitra: What's one of the biggest or most memorable cyber incidents you've dealt with, and what were the lessons learned from that?

Aaron: I can give two examples. One was very early on we had an accounting firm that had just two partners, so it's a very small organization. They had a hacker get in. We actually got the call from another cybersecurity firm who had already been in, and they said, "We're a little bit over our heads. You should give these clients a ring."

Aaron: When we got there, you can think of it as software on two different screens, so on the left screen was the software that that small accounting firm was using to file taxes for their clients. They had between 500 and 600 clients, been in business for 20-plus years. On the right-hand side of the screen was a list, and that list contained the names and social security numbers of quite a few people and sort of check marks on the list of people for whom they had filed false tax returns.

Aaron: What was interesting about the list is that it contained not only people from that firm but from three other firms in three different states. So what we had interrupted was essentially a work bench for a hacker, and that hacker was slowly working through the list of people that he had pulled together and using that firm to file those false tax returns.

Aaron: We got the FBI involved; they were great. We have a really strong relationship with the Bureau and their team is fantastic to work with.

Aaron: Unfortunately, at the end of the day, that organization no longer exists. The cost of the breach and the damage to the trust with that organization, despite the fact that they had 20-year relationships with many of their clients, most of their clients said, "You know what? We think we're going to try and file our taxes with someone else this year."

Aaron: So it was a pretty early lesson in the damage that can be done when somebody gets in and hacks your system and really breaks that trust between a company and its customers.

Chitra: And what was the other story?

Aaron: The other story, there was a large organization that we work with that had individuals in their order entry group that would call back to IT, and it's the usual phone call. They said, "Are you guys doing anything back there, because it's just slow. Things are just slow." And they said, "No, we're not doing anything." "Well, are you backing up?" "No, we don't do backups during the day. Thanks, but please get back to work."

Aaron: This went on for about six months, actually, and they would call the front desk, the front office would call and the IT folks would say, "No, we're not doing anything." Can you do your work? Is your system working?" They'd say, "Yeah, it's working, but it's slow." So this went on for quite a while.

Aaron: Eventually it got to the point where the IT group looked more closely and the system had been compromised and the hackers were siphoning off something like 10% of the resources from this very large server farm. Had they taken 80%, the IT department would have noticed immediately, but because they were only using a small percentage of the systems in that company, it just made everything a little bit slower and they were able to get away with it for almost a year.

Aaron: So we got in, we figured out who they were, kicked them out. Actually, the hardest part of that breach was that we spent a lot of time trying to figure out who else had been invited to the party.

Aaron: Frequently when a hacker takes over a large computer system like that, they'll sell the keys to a number of different people. So they'll sell it to people who were mining bitcoin, cryptocurrency. They'll also sell a set of keys to somebody who steals identities. They'll sell a set of keys to somebody who steals credit cards.

Aaron: So, often times, you won't have just one person in the organization, you may have four or five creeping around in there doing what special area

that they know best, rather than just the classic picture from 20 years ago where a hacker would get in and do all of those things themselves.

Aaron: So that was probably one of the more technical breaches that we've run into recently.

Chitra: That's pretty amazing and scary at the same time. Are you glad that you took the path you did away from academia and that you're doing what you're doing today and kind of looking back on your trajectory from being that young metal singer to performer to where you are now?

Aaron: I love the work. If you're a person that enjoys dependable work environment, a static, predictable day, and you want to know that if you put in a good day's work that in 25 years you'll be able to retire, this is not the industry to work in.

Aaron: For that matter, neither is being a metal musician or working in biotech. There's a sort of theme to all of those things, and that if you're a person that's comfortable with the ground moving underneath you, if you're most comfortable with a certain degree of unpredictability, if you enjoy trying to figure out, all right, so this happened, what am I going to do next? this is a great industry to work in.

Aaron: The things that you learn today may not be at all useful next year, but you learn something new tomorrow and that buys you another day. I think the same is true on all three of those disciplines.

Chitra: Are you still a musician? Do you still perform?

Aaron: I am, actually, and I still play with three of the five people that were in the band. We don't play out.

Aaron: I have to be honest with you, the charge of, the excitement that you get when you're 16 and playing in a metal bar isn't easily replicated when you're 45, so I have to admit I did replace some of that. I got into scuba diving on our honeymoon about, I guess, 16, 17 years ago, and got into cave diving, so cave diving is really where if I'm to take a vacation, that's really what I prefer to do.

Aaron: It sounds a little bit like bungee jumping, maybe, but it's more about managing risk. If you're careful with your equipment, you're careful with your procedures, if you trained well and know the technical things that you need to know, you can make it pretty safe. But it's still pretty exciting stuff.

Chitra: So I guess it's all about managing risk and that's kind of where you are, whether it's avoiding getting killed in a biker bar or cybersecurity risks or cave diving.

Aaron: Absolutely. Absolutely. And what's your acceptable level of risk? Figuring that out for yourself, you know, how much risk am I willing to take? Am I willing to accept the potential downside and is the upside worth it? I mean, that's the same in all of those things. It's a good point.

Chitra: Well it's been great talking to you, Aaron. Do you have any closing thoughts?

Aaron: No, not at all, other than I really appreciate the opportunity to chat and thank you for the time, Chitra.

Chitra: Where can people learn more about you?

Aaron: Our organization is called ProCircular, www.procircular.com. We do cybersecurity and compliance work, and anybody, any organization that's looking to help get their arms around cybersecurity, our company will help you to manage your cybersecurity risk, and we're pretty good at what we do.

Chitra: Well thank you very much for joining us.

Aaron: Thank you, Chitra.

Chitra: Aaron Warner is founder and CEO of the cybersecurity firm, ProCircular, based in Iowa City, Iowa.

Chitra: Thank you for listening to When It Mattered. Don't forget to subscribe on Apple Podcasts or your preferred podcast platform. If you like the show, please leave a review and rate it five stars.

Chitra: For more information, including complete transcripts, please visit our website@goodstory.io. You can also email us at podcast@goodstory.io for questions, comments and suggestions for future guests.

Chitra: When it Mattered is produced by Jeremy Corr, CEO and founder of Executive Podcasting Solutions. Come back next week for another episode of When It Mattered. I'll see you then.