Ted Bauman: Welcome, folks, to another edition of our Offshore Millionaires call, soon to be called Bauman Unplugged. I'm speaking today with Brad Deflin, who is an expert in information security. He has started a company that's providing some very interesting products in that regard.

We're talking about the kinds of strategies that individuals and households can adopt, and small businesses, to protect their privacy, to protect your information, to protect your communications, and so on. So, Brad, welcome – how are you today?

Brad Deflin: I am well – glad to be here today, Ted.

Ted Bauman: Good. Brad, before we start, let me ask you: Have you ever been a victim of information security theft or any problems of that kind yourself?

Brad Deflin: I, luckily, have not. It's been close to me. And in my roles in compliance and leadership and audit and the financial services sector, I could see the fallout of some breaches. But fortunately, so far, no, I have not been a victim.

Ted Bauman: Okay. The reason I ask is because I had some credit card hacking repeatedly last year. I think I was caught up in the Target breach. And I know that a lot of our readers have mentioned that they are. So, that makes you a particularly lucky person.

What got you into information security? You mentioned your background is the financial sector. Tell us a little bit about what got you into it.

Brad Deflin: Well, I think that two common underpinnings to everything I've done in a 25 or 30 year career has entailed risk management on one hand and technology on the other hand. When I first came out of my academic environment and started my professional life, personal computers were just coming onto the scene. I was fortunate enough to have embraced them very early and understood the power that they brought to bear. And so, I was just very interested in being a student of technology and how I could apply it in my professional life, which happened to be around risk management.

And so, in dealing with some of planet's wealthiest families for that matter, in talking about things that could affect them well beyond their acts and allocation, or exposure to financial markets,

it became clear to me about three years ago, that really, their entire face of risk is changing — and that I was in a position that perhaps could do something about it.

Ted Bauman: Right. And now you've started a company, I understand. So, tell us a little bit about that, and the services that you offer.

Brad Deflin: Sure. So, after 25 years in financial services and a variety of positions, mostly senior leadership and management positions – again, those that entail compliance and supervisory type of accountability – I decided to get into this field. It was a very natural transition.

I was dealing with, again, wealthy families that were figuring out ways to negate the risks of any of their environments – professionally, personally, on a family level, what have you. And to me, this was a distinct conversation that needed to be had on a whole other level, in order to add a level of value that they were really looking for.

So I stepped out of the industry, financial services, and into the business of cyber security, but aiming at markets that traditionally had been neglected. The large enterprise, call it corporate, government, and military, public enterprise, private enterprise, and did that for decades in information technology and security.

But anybody out of these large IT-centric server-based architecture environments really was being neglected, even as the risks were elevating all of the time. And their engagement in risks were expanding all of the time. So I stepped out, with really the same target market, the same sector but providing a different aspect of value when it came to risk management by starting a company that could bring tremendous effective enterprise-proven technologies for the sake of information security. But into these new environments that had been neglected before.

Ted Bauman: Now, you also write a blog, I see, on your company site. I think one of the really useful things about that service, the blog, is that it really brings home the risks to potential customers including people like our readers. And interesting to me is that you distinguish between vertical and horizontal information risk. Why is that distinction important for our listeners to understand?

Brad Deflin: Yeah, so I think that is sort of underpinning the fundamental aspect of understanding what's happening. We've been exposed to, and familiar with, the risks at the large enterprise level. And we know

about breaches at the Pentagon and the involvement with the Chinese army, and all these large organizational level attacks that we read about. And that seems to be the primary concern in the area. Now, when the internet was primarily built around server-based architecture and users were in IP-managed environments, again, at the corporation, or the enterprise level, they were being protected.

However, the hackers, whether they be activists or anarchists or corporate spies or government espionage, any of those things, were going after honeypots of information. So they'd come in through a centralized server environment, and reside there electronically for a while to gain the information that they could. Now that the planet is so mobile in its use of computers, the targets have been changing from that vertical server, large enterprise target, if you will, to the individuals and the systems that they use — like cellphones or laptops.

So we would say that's a horizontal target. Instead of one large honeypot type of a target, hackers now have the ability, and the profit motive, to go after lots and lots and lots of smaller targets simultaneously, very effectively and efficiently for profits. So the risk, which has gone from being a cyber-Armageddon type environment, which is still a risk, to one of what the administration and the top security officials in the country call low to moderate risk.

The low to moderate risk, which is more individual as opposed to enterprise, is actually the greatest at risk in the country, according to anybody that is talking officially about the matter. It takes a $750 million dollar economic toll on our domestic economy alone, not to mention the disruption and other elements of friction, if you will, to the system.

And so more attention is being paid, and there's a higher level of understanding that this is a horizontal problem. It's a broad problem. It's a widespread problem. This is not something that we can protect from the large organizational standpoint alone, what I previously referred to as vertical target.

Ted Bauman: Right, understood. So I think it's an interesting point that you make that a lot of us have the tendency to look at data risk as being something that really applies to the big institutions. But the revelation in the last couple of years has been the recognition that it applies to all of us.

On that score, one of the things that our listeners often hear about is encryption. I've written myself in this month's report about disk encryption. I've talked a little bit about file encryption. And of course there's encryption when it comes to communication. But really, that's only going to help you with regard to the information that you have still in your possession. What about the information that's out there in the hands of "Big Data"? What sort of strategies can people use to address the risks of that data? Once it's out of your hands, it's really out of your ability to control. What can you do?

Brad Deflin: To your point to say that information loss is really one way — you can't get it back. And we *are* leaking our personal information. It is being absorbed constantly. The pace of the activity is increasing at just phenomenally alarming levels … every day, unless we turn the faucet off a little bit, by restricting our use of the internet.

I'm a huge believer in leveraging the internet for all that it's worth. I just don't believe you have to leave fear and risk in between you and the world of knowledge and information. So you can continue to use the internet, but by using techniques that throttle back the level of information we use on an automatic basis. Like a virtual private network, for example.

For example, by not using "free email systems" (like Google or Yahoo). Of course there is nothing for free. What you're doing is losing an arbitrage trade, where somebody understands the value of your personal information much better than you do. And in the small print of the contract of the free service, they're taking all your personal information. The problem is that malicious parties can do the same thing. They have the same technology. They have the same types of access to that information.

So we suggest you think about four components.

Number one, protect the device – that's antivirus, and the traditional host of things that protect your hardware that's in your hand or on your desktop that you use it.

Number two, when you are connecting, use a VPN so that everything that goes over – your information, your banking, your shopping, your browsing, your personal information, is automatically encrypted. And it's just white blanks to anybody else.

Thirdly, use a private email account that strips the information that's otherwise available, again automatically.

Fourth, we try to develop solutions to take no behavioral change or at least minimal behavioral change. Just mitigating the risk of e-mail is a huge step forward because it really is considered far more at risk.

And that's where encryption comes into play. None of these things alone will solve the problem. Any of them individually will take a great step forward in terms of mitigating the risk. If you simply put a seatbelt on, you dramatically mitigate the risk of harm or injury or death in a car accident – and so the same thing with some of the solutions.

So then what you've done is throttle back that outflow of information. You become less and less and less relevant to the malicious parties that want to use that against you. Your information becomes stale. And there are missing components to your information.

Essentially, you kind of take yourself off the radar. It does not guarantee that you will not have problems. But it does dramatically reduce the probabilities of having a problem and the negative consequences if you do have a problem.

Ted Bauman: Just following up on that question. I like the very interesting point that you're making, because one of the things that I constantly come up against when I'm talking to people about digital and information privacy is the understandable reluctance to give up some of the benefits. The online shopping, some of the online commerce that really has revolutionized retail trade in the United States.

If I understand you correctly, what you're saying is that the information that you give those big institutions has value when it's combined with other information that you actually don't have to give over in order to get benefits. So it's really about being selective, isn't it?

Brad Deflin: Precisely. And so the way that we have to think about this is that as your information is being collected, it is being curated. And there's very powerful software — big data software that does a lot of work with a lot of data in a very fast, effective, and very inexpensive way.

And what we have to remember is the tools that the hackers are using literally every day get more powerful, become cheaper and more accessible, and can do more harm. As individuals and families and small groups and professionals, we have also to undertake the advances in technology to protect ourselves. Otherwise it's simply a losing equation. We don't have a chance.

Ted Bauman: Now, you mentioned that technology is an opportunity to do something about these things. One of the questions I want to ask you is about tokenized point of sale technology. I wrote about this earlier this year, and I mentioned it a couple of times to my readers saying that on the surface of it, it sounds like a great idea. Things like Apple Pay, where you're really creating a barrier between the actual account information and the information you use to transact.

What do you think of those kinds of technologies? Are they really safer? Or are there hidden problems in them as well?

Brad Deflin: Well, I think both, honestly. They're getting more and more advanced, more and more convenient. And it would be foolish to think that, especially younger generations, will be able to be engaged and productive and thrive in the world without fully leveraging these amazing tools that technology continues to bring us.

But with that, we must have higher levels of awareness. We have to use more discretion, and empower the technology that's out there to our own benefit from a security standpoint. The good news is that's the way technology goes. It gets faster, easier, better, and cheaper all the time. And it will continue to do that even in cases we wouldn't even be able to see at this point in the relatively near future.

So we can condition ourselves to be the beneficiaries of the technologies. And that's what we really advocate here. And so as Apple, or as the innovators, Google, so on and so forth, add services and add technologies to add convenience, and for productivity to your life, you have some level of personal awareness to evaluate them. You know when to put your toe in, and you're also using things that will protect you in the process.

But there will be pitfalls. That's just going to be part of it. We move into a neighborhood, we will ultimately determine where the bad factions, if you will – and how to stay away from those areas. It's just a matter of living in the digital life. Becoming a cyber-

citizen, if you will, which really is going to be required – our generation, most certainly the generations that come after us.

Ted Bauman: I asked that question specifically about these kinds of technologies, because I had written about them. Then people started talking about the fact that Apple Pay in particular was being compromised not by the users, but rather through the likes of setup protocols that financial institutions use to authorize Apple Pay. That reinforces the point that you made earlier, which is that the institutional risks impact people. We need to take those into account. Is there anything that one can do – are there any sort of rules of thumb, for example, when you are using one of these payment technologies, in particular?

Brad Deflin: I think that's exactly what you're looking for: Rules of thumb that you can apply to your decision making. You don't have to be an expert or an IT type of person to navigate your way through this. But I think the rule of thumb here when it comes to these payment processors is, well, who's the underlying party? I think there are certain parties that can be trusted a lot more than others.

And think about if you're undertaking a service that is "free," well, where, really, is the imbedded cost to you? What do I really lose in that exchange? What are the economics? And if it's lopsided, just stay away from it. Or if it comes from a brand that is known to abusive, then you stay from those also. You vote with your feet.

I think this also addresses the point of the need to be both offensive and defensive, right? You need to make defensive distinctions and decisions. But you also, in case something does happen, be able to be offensive in your security technology, in your practices and just in terms of controlling your digital environment, to mitigate the risk of anybody using that information in a harmful way against you.

Ted Bauman: All right, so it really comes back to the common sense angle. Now I'm going to come back to that question of the software side of it – the human brain software side of all of this. But one of the things that I've mentioned to our readers a couple of times, which seems quite attractive to me, are services like Silent Circle, which claims to provide secure communications technology.

One of the most popular things our listeners are thinking about this idea of being able to communicate effectively and safely through encryption. Are those worth it for the average family or small business? Or are there alternatives to something like Silent Circle,

which I get the impression is really oriented towards the corporate market?

Brad Deflin: You're right. We're at a real juncture, if you will, in distinguishing of the corporate user, the enterprise user, the cyber folks who have in the past been in the large organizations that think collectively and makes decisions on a more institutional level. And that's the Silent Circle.

Great technologies have been developed and innovated for those larger concerns in the past, and even without a lot of regulatory pressure or demands from the consumer, they've innovated solutions because they had a certain niche approach to the market. Now, though, environments are being regulated, enforcing official decisions in investment and information security.

And consumers are becoming more aware and demanding more. They want to be autonomous. Privacy's been important to them and they are seeking solutions. It's going to take a different provider than maybe the ones we've seen in the past — the typical places the corporation or enterprise could go for those solutions.

This is our purpose in life, if you will, the total digital security. It would be a platform for this new and emerging market that may not have the resources or the IT expertise to access solutions that they can design for large organizations. But to be able to access those same solutions just in a little bit of a different way.

Because now with cloud environment, cloud-enabled platforms, software- defined solutions, and smart and context-aware type of defenses, we no longer need lots of hardware. We no longer need lots of IT expertise and support and service. We can do a lot of the same things these large organizations require, but in a different way that better address the needs of the individuals as opposed to the individuals going to Silent Circle and trying to figure it out.

And so we think there will be a lot of innovation. And we will be hosting that innovation as it comes, because these new markets need these solutions. And whether they're coming into a regulated environment or not, are beginning to make decisions in investments, and putting themselves in a better spot.

And they need to have access to a different way of thinking about it, distributing it, administrating it, and paying for it. And so security is becoming a service. Where in the past you would buy servers and hardware and support and IT hourly type expenses, it's

now becoming a service. You pay a flat fee. You have a very predictable economic outcome. You always have the latest and greatest and most current solutions. And when you think about security, it's not a transaction.

You can't buy and sell security. You've got to earn it every day. You've got to be vigilant at every moment. And so the service-oriented model is a lot more fitting. And also avails this technology – it's unique, and anybody else that wants to avail it. Make themselves or bring it available to themselves.

Ted Bauman: Well, I'm very happy to hear you include that way of thinking, because one of the things that we grapple with in helping our readers and our subscribers and our members to cope with the challenges to their privacy, is to make sure that it's understood that this not something that you can go buy a product one time, and have the problem be taken care of.

This is a rapidly changing field. In fact, my personal approach is really to create a virtual loose leaf binder for people that I can constantly update to tell them about new challenges and new solutions. So really I think the idea of security as a service is a critical one. In fact, I talk about it as being a state of being rather than as something that you can acquire. So we're definitely on the same page.

Now, as a final question, and I think this probably goes to the heart of the matter, is that in one of your blog posts, you say that cyber security is as much social science as it is technology. Tell us what you mean by that. I think to me that really gets to the heart of the matter.

Brad Deflin: Yeah. So what we mean by that is this – the technology's going to take care of itself. Technology advances in exponential rates. And some people understand what that means. Others might be lost. But the point is that technology advances at levels far beyond what the human does.

We can plan for better, cheaper, faster, and easier to use technology almost every day going forward. It's a natural fact of physics. And so yes, you want to be in a position, like a loose leaf binder or "plug and play," from a solution standpoint, because the environment from a threat standpoint is so dynamic. And the environment from a solutions standpoint is so dynamic. That is great news for the consumer. So the technology is not the problem. The level of awareness, and then the inclination to take action is

where the problem is. There's still a lot of apathy here. So our work is much around the discovery of technology, and the engineering of that technology to bring in to these new environments, as opposed to the large corporation, for example – and to raise the level of awareness and empowerment.

And try to grind away at the level of apathy. And that's where the social science aspect comes in. Then you have to start thinking not in terms of technology, but in terms of how do you communicate to people. How do you create action? And how do you bring about an understanding that things really are different. And in the future will only be more intense.

But there are things and methods to approach it that are highly affordable and very easy to use. You just have to bring yourself to a level of awareness. And then take action. And that's tricky. People don't necessarily respond to risk the way you think that they might. People actually respond a lot more recklessly to opportunity than they do deliberately to risk.

That's just human nature. And so you come into the space of marketing and public relations as well as education and then really thinking about the human brain. And how to bring a different level of understanding that will finally encourage almost anybody to make a decision to approach their life of technology a little bit differently.

Ted Bauman: Well, I'm glad to hear you say that, because I think, as I said, that in interactions with readers, it really has become clear that this isn't the kind of thing that you want to become aware of once something bad has already happened. This is an opportunity people have to address the problem upfront by taking appropriate steps.

Brad, can you tell us a little bit about where people could contact you if they wanted pursue maybe looking at your company and your products – your webpage, for example.

Brad Deflin: Oh sure, so we are Total Digital Security. We're located out of Palm Beach, Florida and Zurich, Switzerland. We're www.TotalDigitalSecurity.com. My name is Brad Deflin, very easy to find and Google. We publish our content to all the online and social media channels. And then our corporate number is 561-833-0846, again, in Palm Beach, Florida. We're glad to be helpful in any way we can.

Ted Bauman: Excellent. Well, Brad, thank you very much for talking to us today. And of course, for our listeners, Brad's contributed a piece to our June edition of Sovereign Confidential. And we'll also include some of the contact details for his company in that publication, as well. So look for that in the mail. Brad, thanks very much. And we look forward to speaking to you again sometime soon.

Brad Deflin: Thank you, my pleasure, Ted.