AESNATION.COM

ACCELERATING ENTREPRENEURIAL SUCCESS PODCAST

EPISODE 82

Marc Goodman

Show Notes at: *http://www.aesnation.com/82*

Dear Fellow Entrepreneur,

We are thrilled that you have joined us here at AES Nation, where we're dedicated to accelerating entrepreneurial success—your success.

We hope you find this transcript to be a valuable supplement to the podcast and encourage you to share it with like-minded entrepreneurs in your network.

In addition to our five-times-a-week interviews with leading entrepreneurs, keep in mind that we have plenty of other resources to help put your success on the fast track:

- Our **monthly live, interactive webinars** co-hosted with Dan Sullivan of Strategic Coach feature today's top entrepreneurs. These are world-changing entrepreneurs who have the insight to help transform your business.
- Our **virtual conferences** showcase business leaders and experts in elevating your success and your life. These one-day online events give you access to the in-depth presentations and interaction that you'd get at a live conference from the comfort of your office or home.
- The **AESNation.com weekly newsletter** will always keep you on top of the latest interviews and events. Sign up here.

Thanks for being part of the AES Nation community. We'll see you online.

Best of success,

John Bowen
Co-founder, AES Nation

John Bowen: Wow. As entrepreneurs, every one of us wants to build fantastic businesses. We want to accelerate our success, and there is nothing that's more powerful in enabling us to do that than technology. It is giving us unbelievable tools, each and every one of us. This podcast, whether you're watching us on video or listening to us on audio, the ability to put tools like this to get it for almost no money at all and to reach unbelievably to our clients and serve them well, but there's a dark side. Really, an evil side. Just as you and your fellow entrepreneurs can use technology, criminals can too.

I have one of the most remarkable individuals who's going to join us today. He's got a law enforcement background that is amazing. A matter of fact, when I first met Marc Goodman, I reached out to him and hired him. I've paid him tens of thousands of dollars for the advice that you're going to get today, so that you can protect your business, protect your clients, and continue to deliver tremendous value. I'm John Bowen. We're at aesnation.com. Stay tuned. You do not want to miss this.

Marc, I am so excited to have you here. You and I have been friends for a number of years now. I've watched your career and just really take off, and you got a new book coming out. We're going to be talking about Future Crimes. It's pretty amazing what you've accomplished and the insights you shared with me, and my fellow clients, my coaching clients and entrepreneurs. I wanted to bring you on the podcast to do that today. First of all, thank you for joining us with the magic of Skype.

Marc Goodman: Thank you, John. It's my pleasure to be here. Really happy to chat with you.

John: Before we go in, I always love the backstory of every entrepreneur, and you've got a little bit more colorful one. I'm going back to the … I'm thinking WordPerfect. Remember the first time you told me how you became this tech genius in the criminal side and the … And really the progression. Before we dive in to all about how this affects us as entrepreneurs and how we can deal with it effectively, I'd love to just have you share a little, the progression of how you became who you are. Now, recognized as really one of the leaders in the world on Future Crimes.

Marc: For me, it all started out with career in public service. As a young kid, I watched a lot of cop shows on television. I saw the cops walking around the neighborhood in New York where I grew up, and I said, "Wow, that's cool. I'd really like to be part of that;" so I applied, and went to the Police Academy, and became a police officer, worked in a variety of assignments. I was a patrol officer, a supervisor, and a detective, investigator. During those early days, I got lots of cool cases; but one of the things I noticed is that bad guys were using technology too.

One day, I was working as an investigator, and my lieutenant screamed my name across the detective squadron, "Goodman, get your ass over here." I'm like, "Okay, boss. What's up? What did I do?" He said, "I got a question for you." I said, "Yeah?" He says, "Tell me, do you know how to spellcheck in WordPerfect?" I said, "Sure, shift-F2." He smiled, and going smiled. He said, "I knew you were my guy. I got a case for you. It's a computer case, and you're the only guy that can handle it." As it turns out, knowing how to spellcheck in WordPerfect made me amongst the technical elite of cops back in the day. From there, things just took off.

John: Marc, what year was that?

Marc: That would have been 1995 or so, so it was very early days for …

John: Really, the internet. It was there, but it wasn't being used by us as entrepreneurs very much, and certainly the criminals yet. Give a little of the progression that you did just so because it's one thing to have been … It's great to have been, be a cop to serve the public as you had, progressed and became one of the senior technology … In one of the major cities, but you didn't stop there.

Marc: No, I was very, very intently curious. I went back to grad school at Academy School, learned more about science and technology. Took some classes at MIT as well to learn about … From the business school there at the Sloan School of Management. At the law school, to learn as much as I could, and then, I went and founded the Internet Unit for the Police Department. From there, I went to London. There at London School of Economics, there was a computer security research center there that I was at.

Then, I got recruited into INTERPOL, the International Criminal Police Organization, and I spent about a decade working with them on international organized crime around the world, trying to help police get up to speed on these issues and helping them track down bad guys in more than 70 different countries. From INTERPOL, I did a few other things. I worked with the US Secret Service in New York on the Electronic Crimes Task Force, worked with the FBI as their futurist in residence. After that, back in 2010, after 20 years of government, the light bulb finally went on, and I said, "Hmm, government. There may be something else out there for me."

After 20 years, I decided to jump shift and become an entrepreneur, moved to Silicon Valley, ensconced myself in that culture, learned as much as I could about the technology, and … Because I had always approached these issues from the policing side, from the national security side, so what was interesting is building up my experience and expertise on the tech front. No better place, obviously, than Silicon Valley, and that's where I brought it all today.

John: I'm going to put one more piece in because we were together recently at Peter Diamandis' Abundance 360, and Peter Diamandis and Ray Kurzwell put together a university, Singularity University, and they wanted you bad to be there to share. This is … All of you, anyone listening or watching this should take a look at Singularity University and what they're doing. They're just bringing the best minds together on the future. As entrepreneurs, we can create the future if we know the trends that it's going. It's largely technology, but they've asked Marc to lead this part as well and just … I hear nothing but great things of what you're doing up there.

Marc: Thank you. I should point out Singularity University is awesome. It's co-founded by Peter Diamandis and Ray Kurzwell. Google and NASA got together and created this school, so to give you the sense for the power behind it. Housed on the campus of the NASA Ames Research Park. Our instructors are roboticists, and synthetic biologists, and astronauts, and big data scientists. You have some of the biggest and brightest minds in the world coming together to use all of these technologies that you mentioned when you opened up the podcast for the greatest possible public good.

My take on all of that is very much the same, but I'm the guy that knows a little bit about the dark side, and so I talk about the downsides of this technologies, and try to let the students at the university know that there's a flipside, and what some of those dangers are, and how to prevent them.

John: Let's dive in to that because that's what really what all of us care here. No one is going to be more qualified than you to do this, and I want to make sure we get it from you, Marc. When we think about in today's world, we're just so interconnected. Why don't you talk about how that interconnection because most people understand, "Well, I've got the internet. I can connect. I got Facebook, and Skype, and all these different social media sites. I've got my email and everything. They know on the surface what's going on, but they don't really know what's going on deep.

I'm going to say, for someone like myself, I know a little bit more. I'm reading your book, and we'll go over your book in a little bit. You're taking that a little different spin. I'm looking at it from a marketing perspective or sharing. It allows me to communicate with people I can serve and so on, but we're collecting vast amount of data. I don't think most people understand what's really going on in the background.

Marc: Absolutely. As you mentioned, the obvious upsides of technology are manifest, right? It's so helpful in so many ways. I want to be really clear that my goal here is not to poo-poo technology or talk to them. I think it's awesome. I think it's amazing. Besides the work that you're doing, it will help us strive amazing change in the world, whether it's radical life

extension, curing diseases, reducing infant mortality, bringing billions of people out of poverty. Technology is great, but there is this ominous flipside, and it has a lot to do with connectivity.

The fact to the matter is, is that we are connected to people all over this planet, and some of them, we might not want to be. Just to put it in physical world perspective, in the old days, if you would, parallel to California or Brooklyn, New York, and we're walking down the street, you might have to worry about being robbed by a crook in your neighborhood either with a knife or a gun.

Now, thanks to the benefit of technology, the crook no longer needs to be collocated with you. As you're sitting in front of your computer or on your smartphone, somebody in Kiev, or Lego, or El Salvador, thousands of miles away, can just as easily get into your life, and steal your money, and cause you harm. The connectivity is on our computers, they're on our smartphones, but it's in so many other things that people don't realize, even beyond our social networks.

John: Yeah. Marc, I was thinking when you're saying … In Russia, somebody doing … Last year, my controller shot me an email and said, "Hey, it's great you're going to the Super Bowl. Hope you enjoy." I sent an email back, and I said, "I'm not going. Why would you say that?" He said, "Well, you just spent $10,000 on tickets," and the …

Marc: Somebody just spent …

John: Yeah, in American Express. I was talking to him because I said I was very interesting in this thing, and they said, "Yeah, no." They had some Russian group had charged a buck on my credit card, random numbers, to make sure it was working, and then hit 10,000. We were able to cancel it because my controller was reviewing bills. It's amazing. You don't think of that. It's like you're violated, and we're seeing … We've got tons of stories where it just happened to me, and friends, and everything; and then we've got some big media side, but it's just … We're so interconnected now, we take it for granted.

Marc: Absolutely. By the way, just to point out something that happened to you to help your guest be informed about this, that methodology of the $1 charge, $1.50 charge, that's criminals testing your network. They're testing your number. They're testing the pin code. They're testing it to see if it goes through. Once that goes that through, then you get hit with the big $5,000, $10,000 charge after, so very common. Beyond all the technologies of today, there is a tsunami of technology coming down the pipe that most people don't realize. All the things in our life that used to be physical devices or mechanical devices are turning themselves into information technologies, right?

Marc Andreessen famously said software is eating the world, everything is becoming software or hardware. For example, the printer, the one that Gutenberg created, used to be a physical device. Now, it is a computer. That car that Henry Ford created and put off the manufacturing line, those are computers. The average modern automobile has 250 microchips in it. It controls everything from your airbags, your braking, your car stereo, your windshield wipers, and those 250 microchips can and have been hacked. A car today is not just a mechanical device. It's actually a computer that you ride in.

An elevator is a computer that you ride in. An airplane has a Solaris box that you fly in, and we're even taking these computers and putting them inside our bodies. Pacemakers, defibrillators, cochlear implants, diabetic pumps, those are computers that we put into our bodies, and they're all hackable. The subtitle of the book "Future Crimes" is "Everything is Connected, Everyone is Vulnerable, and What We Can Do about it." Just one last point on the number of connections, people think today that, yes, we have the internet. It's ubiquitous. We have 2 billion people online, but internet today is tiny. We are at the earliest minutes of the earliest hours of the earliest days of the internet. It will explode.

Today, we use Internet Protocol Version 4, IPV4 for short. In the next few years, we're switching to Internet Protocol Version 6. That means that we are going to go, metaphorically, from an internet today that seems so big, but it's metaphorically actually the size of a golf ball to an internet the size of the sun. That means a huge growth. The more things that are connected, the more things that are vulnerable.

John: Marc, it's not only the more things connected, as you've taught me, it's the more people too. When we … I was just reaching over like grab a hold of my smartphone, and the … I have an iPhone 6 at this time. I probably had 1, 2, 3, 4, 5, 6 along the way, and some Android phones too. The power that I have there, the interconnected that you have, and now we're going to have … We can debate how many years, but we're going to have another 3 billion of these 7 billion people in the world.

They're skipping a whole bunch of technology, and all of a sudden, they're going to have smartphones too. It's amazing, the opportunity. As entrepreneurs, either they're going to be our customers or they're going to be our customers' customers. It's going to have a huge amount effect.

Marc: Or your competitors.

John: They're going to be our competitors. IT's going to be a lot of wealth creation; but also, that vulnerability part. There is a lot of people coming online with some really sophisticated tools, and we're all interconnected.

Marc: Yeah, and that smartphone that you just held up. Most people don't realize the power of Moore's Law. The fact that the power of technology is doubling every 18 months, so that means 18 months from now, your computer will be half the price and twice as powerful. That iPhone that you just held up, believe it or not, had more computing power on that one iPhone in terms of processing power of the chip than that was available to all of NASA during the Apollo 11 launch. You have more computing power in your hands than all of NASA did, so the next obvious question is, what will that iPhone be like a few years from now or 10 years from now?

John: No, and it … Really, I want everybody to take what Marc just said that Apollo 11, going to the moon, versus where you're just walking around within our pocket this power. It's not only us. I believe there's about close to 3 billion devices or people using. I think there's more than that … Devices out there now.

Marc: There are more devices than there are people on the planet. All of it. There are more than people on the planet.

John: When we look at this, and this is just … I get so excited about technology, the opportunity, it allow … It enables us as entrepreneurs to really magnify. Once we get … Nail a client experience, whatever we're delivering, the ability to scale it up, and create systems around it, and the global world as our client, this is great, but they're … It makes more vulnerable. Marc, lets' talk about … There's some recent press that's going on. I'm thinking two big ones. One, I have couple … I have a Black Card because I travel so much, Black Card with American Express. I have a Palladium Card with JP Morgan. They're expensive cards, even produced in their little marketing gimmick and all that.

I can remember when Target happened. As a consumer, it's such a pain, but both those companies sent me their big packaging, and made it dramatic of how they're protecting me, and gave me a new credit card. There so much backstory behind it and what protection is going on. Maybe start with Target. How did that happen? Yeah, this is a really good business. These people are responsible. They're working hard on this. How could anything like that happen in today's world?

Marc: It actually goes back to that point that we were just discussing of our interconnection. What happened in that case, with the Target case, two Christmases ago now was that the point of sale terminals where everybody swipes their credit cards, those were hacked. Think about those little terminals. What are they? They're just small computers. They're hardware and software, and somebody was able to get into that. How did they get into? Did they go to a hundred Target stores and hacked each device of the hundred checkout registers that they had individually? No, they did it on the internet.

Here's the fascinating thing that people wouldn't realize. For your podcast listeners that are business owners, just to show the power of that interconnectivity and how it can make us vulnerable, how did they get into the Target point of sale terminals? Via the air conditioner. What? Yes, via the air conditioner. As it turns out, Target used a third-party contractor to manage their HVAC systems across the whole country, and one guy at that company clicked on an email that had an attachment on it.

He downloaded the attachment. It infected his computer, and then that was used to get into the heating and air conditioning systems. From that, they were able to get into the Target vendor system. From that, into the main Target systems, and eventually climbed all the way through to the individual cash registers. By the way, that attack was carried out by a 20-year-old kid in Russia, so once …

John: It's amazing.

Marc: You said, you mentioned that you got a new credit card, you aren't alone. Over 100 million people were impacted by that. What does that mean? That means that one 20-year-old kid had the power to affect and rob 1/3 of American. That's the paradigm shift in crime that people don't understand. We went from that old school robbery, guy hiding in an alley, a dark alley, with a gun or a knife, and robbing one person at a time to now robbing 100 million people.

We've solved the fundamental challenge of crime, which I would say is probably the fundamental challenge of all the business owners listening to your podcast, John, which is how do I scale and grow my business? Criminals could only rob a few people a day. Now, they can rob … One criminal can rob 100 million people. That is a game-changer, and that's why we're seeing these fast cyber-attacks and threats that we have this day.

John: Let's do one more high-profile, and then I want to go one example that touches everybody as well. These high-profile ones make the press, but there's a lot of them that don't make the press. Let's go to Sony. This is … Just the amazing, the amount of damage that was done to a company's reputation, business line, and this is … Target reacted reasonably well. I think we can debate the level as we're all learning how to deal with this. Sony, not so sure. It took them a while to recover on this, but how …? Tell us a little bit about what happened behind the scenes.

Marc: Sure. In my book actually, which was written and turned into the publisher before the latest Sony hack, right, which took them at a stage when they were printing the book, I still had 25 references to Sony in the book. Now, I'm talking about what allegedly happened with North Korea, but just all their other hacks against them. The biggest one being the 2011 Sony PlayStation hack. In that hack, over 110 million accounts were compromised. The Sony

PlayStation network went down for three weeks. The chairman of Sony appeared both before the US Congress and the Japanese Diet. He had to bow before everybody and apologize.

Sony is an excellent victim, okay? There are lots of people who are … You mentioned Target that recovered quickly. Sony as a company has really pissed off hackers, and they're doing it because of their digital rights management. They've been very aggressive in going after hackers, and the hackers are fighting back, and so they are perineal victim. If you look at how they handled that attack from the crisis management perspective, from a preplanning perspective, from the response respective, it was a textbook case in what not to do. Okay? So, so many missteps.

I actually was interviewed by The Economist, and I talked about this. If you would think of any company that should be prepared for a hack more than anybody else, it would be Sony because they have this legacy of massive breaches. It was not done well. You have different parts of the company issuing different press releases that said different thing. They said they were going to pull the movie. They caved to the hackers, and they agreed not to pull the movie. They were criticized by the [crowd then 00:22:16]. Everything that could go wrong from a PR perspective, from a branding perspective, and from a financial perspective did go wrong.

To your question of what exactly happened, basically, back in late November of 2014, as tens of thousands of Sony Picture Entertainment employees showed up at their desktops around the world and turned on their computers, they were met with this banner ad on their machine that basically said, "You've been hacked." Rather than seeing the Sony logo, they saw the logo from a hacker group calling themselves the "Guardians of Peace". The Guardians of Peace went in and took over the entire Sony network. It was on their desktops, it's on their mobile phones and alike.

Obviously, that caused them to freak out. They called in the FBI. They took on the investigation. Ultimately, many people assessed, including the US government, the president, the NSA, and the FBI that North Korea was behind this attack. The reason why North Korea allegedly attacked was because of the movie called "The Interview" in which two comedians went ahead and depicted the assassination of Kim Jong-un, and so the North Koreans weren't going to have all of that.

We can talk about whether or not it was North Korea. I certainly have some doubts about that, but let's talk about what the impact was on the Sony Corporation because for your business, customers, and listeners, the same could happen to them. Basically, the Sony hack showed how desperately vulnerable we are and how extremely dependent we are on technology. As a result of the hack, all of Sony's network, its computer infrastructure were hacked including its telephone infrastructure.

That meant that Sony employees for weeks, and weeks, and weeks could not use email, could not log on to their corporate Sony email. They were all told to generate Gmail accounts, right? You got all of Sony now communicating via Gmail. They were told not to use their smartphones, Apple or Android. Instead, they were told to pass messages to one another on pieces of paper and to revert back the fax machines. They used a sneakernet and a phone tree.

When the chairman of Sony Pictures Entertainment wanted to get out word to tens of thousands of employees, each employee was given a list of telephone numbers and told to all 10 friends, and then 10 friends like that old game telephone in high school. In terms of the impact, Sony made so many mistakes. I don't want to blame the victim here. I get that information security is hard, but they did so many rookie errors. For example, they kept the social security number of 47,000 employees unencrypted on somebody's hard drive. All of that data was taken.

They had a Word document with everybody's password in a word document entitled "Password List", okay? Completely unencrypted. Worst of all, they stored their employees medical records in an unencrypted computer on the Sony network. The hackers released the name of individual Sony employees and noted that they have cancer, that they were being treated for depression, all of this stuff. All of this data that the company didn't even know that they were keeping leaked. Then, of course, their scripts leaked, their movie budgets, films, the new James Bond movie. It all leaked, costing them hundreds of millions of dollars in intellectual property cost.

John: One of the things I want everybody to take a step back to is that the reality is that we're all vulnerable. We're giving two high-profile cases. I gave my little one. We've had a number of different things in my businesses and so on, and have many entrepreneurial friends, small, mid-size businesses that have had some real disasters that have knocked them off for a week or two. One of the things, Marc, I want to go to is because we could go on and on, story after story, but what do we do to protect ourselves?

What are some of the steps that we can do as entrepreneurs to really be smart about this? We can't protect … I have one friend who won't connect to the internet. He's just totally convinced that that's going to attack him in life, but that's not an option for the vast majority. What are some of the steps we should take?

Marc: The great news is, as you said, we can go on and on, and talk about all the hacks out there, but there are a tremendous amount of things that businesses and even individuals can do. In the book, I have something called the "Update Protocol" where I take people through all of these steps, and it's a testing methodology. If you follow the Update Protocol, it's been tested and reviewed by the Australian government. Their Administrative Defense uses it, and

it shows that it can reduce your internet threat profile by 85%. It actually makes a quantitative no difference, and I put all of that in the book.

For businesses in particular, are few things that I can recommend. One is you should create an open-source intelligence program on your company. What does that mean? There are people that are discussing how to hack your company, how to hack your executives, your intellectual property is showing up online, your client list, all of that information is leaking, and the challenge is, is that most people, most companies don't know about it until it's too late.

The very simple version of this is just creating Google alerts right on your company to see if hackers were talking about it, where it might show up. For larger companies, they can use third-parties or build their own in-house team to do that, to actually actively monitor hacker records and things like that in the digital underground. Make sure that you're paying attention because bad guys are discussing how to hack you and how to get in there. That's one thing. The second thing is you need to red-team and test your assumptions.

What's "red-teaming"? It's actually a term that dates back to the military, for military exercises, right? America was considered the blue team. The red team were the soviets, right? The Russians. The red team would go up against the blue team and try to break into the America or launch warfare. Every day, the bad guys are in your systems. Most people don't realize it, but a study done by Verizon and the US Secret Service showed that 75% of corporate systems could be penetrated within 15 minutes, right?

Another study said that the average time to discovery from the time that hackers break in to your network until you discover them is 211 days. That means, for 7 months, the bad guys were roaming around your network, copying everything, seeing what it is that they want to take of yours, and you have no idea. The old model of cybersecurity was building big walls and keeping people out. It will build tall fences and motes, and will block everybody from coming in. That does not work anymore.

Your assumption should be, and I believe this whole-hearted, and the FBI Director has mentioned this, they're already there. The barbarians are not just at the gate, they've overrun the castle. The new methodology is you need to go after them and proactively hunt them down because they're living there, so red-team exercises. Whether you do it with people in your own company or you bring in outside experts, you should try to break your own systems to see if you can and see what you can learn because the bad guys are already doing that. Another thing … I'm sorry. Did you have a question?

John: No. Go ahead, Marc. This is great and really very valuable.

Marc: Yeah. Another thing to keep in mind is that you need an adult in charge of security, right? For medium-size, even large corporations, there may be a chief security officer or chief information security officer, a CIO, but many of those people certainly don't have the background to understand bad guys. They're great people. They spent their whole year in tech … Their whole career in technology. Maybe they started out at the helpdesk, and they've worked their way up, and they're very sophisticated. They have degrees in computer science, but they don't understand criminals, and you need somebody who understands criminals.

You need somebody in charge of your risk management and security who's as good at their job as you are. The big problem is that most companies break that down into groups, so they take the head of the CIO, and they make him in charge of IT security. They may have an old retired police officer or FBI agent that they put in charge of physical security, the guards, the gates, the guns, the employee badges; and then they take the head of HR or people, and they put them in charge of background investigation, personnel security. Often, there is very little coordination and cooperation. You need somebody who's got a 35,000-foot view of your security.

Those would be the main things that I'd recommend, but there's one bonus tip I want to mention for businesses of all size, and that is where you store your money. People don't' realize that the rules and regulations regarding personal bank accounts and business bank accounts are govern by two completely different sets of law. For a personal bank account, you'll have FDIC Insurance. They will protect you in case of loss. With most personal bank accounts, you'll have up to 90 days to notice somebody taking money out of your bank account as your controller did, John, with the $10,000 Super Bowl tickets. You got 90 days on a personal account.

Business bank accounts however aren't almost exclusively covered by UCC, the Uniform Commercial Code, which means that those 15 pages of agreement you signed in 4.5 when you opened up your bank account, hidden deep in there, it said, "If there's a dispute on your bank account, if you are hacked, if the money is missing, you have 24 hours in which to notify the bank." If you don't notify the bank within 24 hours, then you're taking the loss. Criminals have realized this.

In the old days, they would go after people's personal bank accounts. If you ripped off 10,000 customers in Citibank, Citibank's got a whole team of folks that are going to go after the hackers that did that; but on the business bank account side, there's no need for Citibank to send their team of investigators on it because your company is the one that's going to eat that loss. We're seeing around the country small, medium businesses having losses of $400,000, $500,000. It's affecting school districts. It's … Drycleaners, doctors' offices, volunteer fire departments, and they're on their own.

Most companies don't have the cyber insurance emplaced to help some of that risk mitigation that meant to help and ease some of that pain. I would recommend talk to your tax guy to make sure you could do this, but do not keep huge amounts of money, millions and millions of dollars in your business account because bad guys are going after. If you do, do that, make sure that you get an alert. You can set this up with your bank that if more than $1,000, $10,000, $100,000 … Set the level that makes sense for your business. If that moves, you're immediately notified, so that you can take action.

John: Yeah, I know. I've been affected by this too, Marc, so this is a really important one. We have really good systems. I grew up on the financial side, and the banks do honor the letter of the law, but at the very tight letter of the law too. We're able to get reimbursement on it. It was a six-figure dollar amount, so it … This can be a matter very, very quickly. Let me go to the next segment. This is the book of the day. We've given four key recommendations. They're great. Your book … A matter of fact, let me put it up. Tell us a little bit about what's in the book first.

Marc: The book is called "Future Crimes". It's coming out by Random House Doubleday. It talks about all of the threats that we just mentioned, everyone is connected or everything is connected, everyone is vulnerable, and what we can do about it. It will take you through amazing stories, right? It's written as narrative nonfiction. It's meant to be fun and interesting. I didn't want to bore you with just statistics or too much science and technology. It's eminently approachable, and so it's got the vibe of technology mixed with crime thrill.

John: Let me bring it up because I will put it up, and I'm going to recommend everybody read this because it's one … Part of me, Marc, when I … I read it. I got a chance to read at The Galley. I was going … Really, it's a great read because it's a little bit … It almost reads as fiction, and then you got to remind yourself, and it's some great stories and so on. It will scare you a little bit, but it will make you much more aware of what's going on, talking about blackouts, and robot bods, and all this stuff, and many of the things that I knew because I'm in Silicon Valley as well.

What I really liked is it tells us what we can do about it, and we can't go over the whole book, obviously, today, I got to tell you, Marc. One of the things, I paid you tens of thousands of dollars to help protect my business as well as my clients' businesses. For $20, this is a pretty good deal.

Marc: I'm glad you think so. It's a lovely birthday gift. It's good for quinceañeras, bar mitzvahs, Diwali, Kwanzaa. It makes a great gift.

John: No, and it really does. I'm going to encourage everybody to go out and get it. It is one. A matter of fact, I just bought. I told Marc to ship me a whole bunch of books for all my clients.

I'm making this as a gift because it is so valuable. With that though, Marc, let's go to the next step on your smartphone. The next segment. What's the application of the day? What are you recommending?

Marc: We all struggle with passwords, right? The average person has more than 20 or 25 different logons for their social media accounts, their bank accounts, their email accounts, and we simply can't remember them all, so we choose silly passwords like "12345" or "password", and obviously, we get hacked. There are actually excellent tools out there that can help you manage these passwords, and they're called "Password Wallets".

There are three different companies that I will recommend. One is called Dashlane, one is last LastPass, and another one is called "1Password", the number "1", and then password. What they allow you to do is set one really long master password, and then you can store in an encrypted format all your other passwords that they can manage on the fly, so you can have both great security and convenience at the same time.

John: Yeah. I love … I use LastPass, but any of them are good, and that you feel like you've actually made a lot of progress, and it's easy to use. Because one of the big things of having long passwords, Marc one time shared with me on my iPhone that I had to have an 8-digit one for security, which really made sense, so I did; but every time, I had to type in the eight. It's just a long one. Now, with the fingerprint on the iPhone 6 and some of the Androids, LastPass, it becomes really effortless.

What I love about what you're doing Marc is you're making easier and easier to protect yourself. It's so valuable. Let me go to the last segment, and that's resources. Marc, I want to pull up your website here. What do you have on marcgoodman.net?

Marc: On my personal website, marcgoodman.net, you'll see lots of stories that I've written, whether it'd be for Wired Magazine, The Economist, Atlantic Monthly about various hacks, computer threats, and the things that people can do about them. On futurecrimes.com, you will see where the book is currently listed. We're going to be posting a whole bunch of information on how people can protect themselves. I talked about that update protocol. That will be available there.

If you signed up at futurecrimes.com, I will be sending out monthly tips on how to protect your kids online, how to protect your business, how to protect yourself on social networks, how to protect your smartphones and alike. In both places, you can find good information. The last place you'll find me is on Twitter at @FutureCrimes, where I'm twitting out breaking news of things you can do. The goal with all of this, John, and you've pointed out, it's education. It's empowerment.

Yes, some of this stuff can seem both daunting and scary, but as I mentioned, there are tons of things that you can do. My goal is not to frighten. My goal is to empower you, so that you in your own businesses and in your own family life can use these awesome and amazing technological tools to the greatest possible benefit. That's what I'm hoping for.

John: Now, that's great, Marc. Let me go to the last segment. I'd like to just summarize the key takeaways. To me, what we need to recognize … This is the subtitle of Marc's book, everything is connected. There is no privacy. It is dead. We are connected. Both, all our data is out there. It's easy to find us, the whole thing. Everyone is vulnerable, so we got to start thinking of these protocols and be very thoughtful about doing it. Marc gave some great suggestions. The book has phenomenal ones.

They are not … It's not 100 pages of recommendations. It's very thoughtful, step by step how you can do it, so that you can protect yourself, your family, your business. Really, everyone you love, and make that difference, and be an extremely successful entrepreneur. What I'm encouraging you to do, go buy the book. You're going to be glad you did. Your teammates, everybody will be because you're going to be protecting them and your family. With that, your clients, your future clients, they're all counting on you. Don't let them down. Execute, execute this. All the best.

A Second Opinion on Your Finances

A Complimentary Service from Financial Advisor Select for the Members of AES Nation

Dear Fellow Entrepreneur,

Like many members of AESNation, I'm a serial entrepreneur. In addition to co-founding AESNation, I'm the founder and CEO of Financial Advisor Select, a firm dedicated to helping successful people make informed financial decisions by introducing them to top financial advisors.

If you're like many successful entrepreneurs, you and your family already have a relationship with a financial advisor. You may even work with several financial advisors. If you are completely satisfied with these relationships and confident that your finances are on track toward helping you achieve all that is most important to you, we congratulate you.

However, you may not be entirely satisfied. You may be wondering if there's a financial advisor who is better-suited to address your family's very specific financial challenges. If so, you are not alone. In today's uncertain economic climate, many successful entrepreneurs are wondering if they have the right financial advisor.

To help you find out if you are currently being served well, Financial Advisor Select is offering a complimentary second-opinion service to all qualified members of AES Nation. Simply contact us to schedule an exploratory call with one of our personal financial concierges. We will introduce you to a financial advisor who we believe has the ability to address your particular needs. The financial advisor will then meet with you and provide you with a second opinion on your finances. There is absolutely no cost or obligation to you.

Find out more about how Financial Advisor Select can help you and your family.

Why do we offer this service? Because at Financial Advisor Select, we have just one purpose: to help successful individuals and families achieve financial peace of mind by connecting them to top financial advisors in their communities. We look forward to assisting you.

Best of success,

John Bowen
Founder and CEO
Financial Advisor Select