The Future of Work podcast is a weekly show where Jacob has in-depth conversations with senior level executives, business leaders, and bestselling authors around the world on the future of work and the future in general. Topics cover everything from AI and automation to the gig economy to big data to the future of learning and everything in between. Each episode explores a new topic and features a special guest.

You can listen to past episodes at www.TheFutureOrganization.com/future-work-podcast/. To learn more about Jacob and the work he is doing please visit www.TheFutureOrganization.com. You can also subscribe to Jacob's YouTube channel, follow him on Twitter, or visit him on Facebook.

Jacob Morgan: Hello, everyone, and thanks for joining another episode of the Future of Work podcast. My guest today is Marc Goodman, who is the New York Times best-selling author of Future Crimes: Inside the Digital Underground and the Battle for our Connected World. He's also a global strategist and consultant focused on the profound change that technology is having on security, business and international affairs. Marc, thank you for joining me.

Marc Goodman: The pleasure is mine. Thanks for having me.

Jacob Morgan: All right, so we're going to talk about all sorts of really, really cool stuff but before we get into any of that, why don't we talk about you. What's your background? How did you get involved with all these future crime business?

Marc Goodman: Let's see, well, I was born at a very early age, like a lot of people. Joking aside, my background broadly is in law enforcement. I started out as a police officer and did that for many years, worked as an investigator, and from there, went from being a local cop with the Los Angeles Police Department, working there for many years, on to working with Interpol. Going from local crime to more international crime, and spent many years working with Interpol around the world on high tech crime, and after that, did some work with both the FBI and the U.S. Secret Service, also focused on high tech crime and on terrorism as well, so broadly, in law enforcement and counter-terrorism. Back in about 2010, I went to Silicon Valley because I realized that the bad guys were out innovating the good guys, and I wanted to go to the heart of the world of technological innovation, and of course, that brought me to the Bay Area.

Jacob Morgan: Why the whole cybercrime space? Was there something specific that drew you to that or a specific moment in your life when you're like, "Oh my God, I got to get into the whole cybercrime stuff," as opposed to more of the traditional crime and law enforcement?

Marc Goodman: Yeah, it's a great question. I actually started out doing all the basic type of stuff. I started out as a patrol officer. I worked vice and narcotics, and doing all the standard police fare and enjoyed it tremendously. When I began my career in police officer, I started to notice criminals were using tech and they were using tech better than the cops were. Criminals have always been early, early adopters of technology, and I certainly saw that when I was on patrol. Bad guys had pagers long before the general public did. Back in the time, in the late 1980s, the only people who had pagers were doctors and yet, drug dealers and gang members had pagers early. Before any police officer I knew had a cellphone, drug dealers and pimps and others were using cellphone technology, so in order to keep up with the criminals and their rapid adaptations to new technologies, I realized that I had to learn about it myself. I did all the standard stuff but I always was particularly fascinated by the way that criminals innovate, so I focused quite a bit on new methods of criminal innovation and technology has been central to that.

Jacob Morgan: Today, when you're not on an airplane, I think you said you're based near the Bay Area or in L.A., but what's a typical day like for you, in the life of Marc? Are you up at 5:00, 6:00 in the morning? Do you have some specific routines of what a day looks like for you or is it just chaos all the time?

Marc Goodman: It's chaos all the time. Entropy is the natural order of things in the world and it's also the natural order of things in my life. It's quite a variety, so one day I could be giving a keynote address to 10,000 people in Vegas about what they or their companies can do to protect themselves, and another day I'm working with a law enforcement agency in the United States or overseas, about how they can go ahead and iterate and innovate to keep up with the pace of change in policing and technology, and another day I'm just giving a lecture to a bunch of high school kids about what they can do to protect themselves online. In between all of that, I do a fair amount of research about all the latest trends, both on the positive side and on the negative side, so I work with some amazing people at Silicon Valley Singularity University. I have friends who are literally astronauts and roboticists, and geneticists, and synthetic biologists, and I often shadow them and take in all the latest, greatest changes that they are discovering, and then, circle around and see how that can be used and abused by other people in society.

Jacob Morgan: Then, you got to find time to eat and exercise, and have a life.

Marc Goodman: That would be useful. I haven't found time for that yet, but yes, it would be very useful to find that time.

Jacob Morgan: So, no eating, we would just plug you into an IV and ship you off to wherever you needed to go.

Marc Goodman: Yeah, exactly.

Jacob Morgan: That's the way that we're going. All right, so I know a lot of people are really interested in the whole privacy and security issues, especially as it pertains to how we work, but maybe if we start from a macro level. Can you give us a sense of how crime has changed over the past few years? What is so different now versus crime 10 years ago, 20 years ago?

Marc Goodman: That's a really interesting question and it's one I think about a lot, because crime is changing, and it's changing tremendously in ways that the general public doesn't understand and that also, that law enforcement and government do not understand. If you look back at crime over the generations or over the past centuries, there have been a few key changes. The first is location and the second is connection. When I talk about location, in the old days, meaning 1850s, you could be pretty clear on the fact that the criminal, the victim, the police, the judge, and the court, and the prosecutor [inaudible 00:09:51] be co-located. Even 25 years ago, if somebody committed a carjacking, we knew that they had physical contact with the victim, we knew that the police were going to investigate it with the local police force, somebody walks into a bank in midtown Manhattan and holds up the bank, it's very clear who the cops are going to be, who the prosecutor is going to be, that the victim and the police are all co-located, which made investigating crime really easy, in retrospect, because all the evidence was local, all the jurisdiction was local.

Now, that has completely changed with the advent of the Internet. The overwhelming majority of crime that takes place today is committed over the Net and is non-local. What that looks like is, somebody in Moscow can hack into a computer system in [San Paulo 00:10:45], Brazil and from that system, break into another system in Kyoto, Japan, and from that system, ultimately attack somebody in San Francisco. The person who loses the money is in San Francisco, the person who perpetrated the crime may be in Russia, and all along the way, in Kyoto and San Paulo, you have evidence that needs to be gathered by different police departments and different jurisdictions and different courts, and different prosecutors. In effect, those systems work really, really poorly and really, really slowly. The ability to frankly get evidence like that can take years, two or three years to collect all that evidence, and yet, the criminals can change their IP address in a matter of seconds, so you no longer have co-location of victim, criminal, and evidence, which has really broken the criminal justice system because that San Francisco police officer has no authority whatsoever to make an arrest in Moscow.

I've said before, that the Internet has broken policing, and it absolutely has, but neither the general public or the cops have realized it. Now, of course, there's still local crime but increasingly, given your chances of getting caught, very few people, or smaller and smaller numbers of people are committing local crime and that's why we've seen this mass increase in Internet and technology-based crime because the chances of getting caught and prosecuted are infinitesimally small.

Jacob Morgan: What's the most recent example that you think the public might be familiar with of some sort of a cybercrime? I know we heard of Target, we heard of Sony, was there anything that even happened more recently on a large scale? What was the-

Marc Goodman: I would say probably the big one in the past 30 days has been the Equifax Hack-

Jacob Morgan: That’s what I was going to say, Equifax.

Marc Goodman: Where over, yeah, over 150 million Americans have their credit files released. It was really bad, bad news. I wrote about Equifax in my book previously, because they have generally been an incredibly poor steward of public’s information. They’ve been hacked numerous times before. The other credit bureaus have been hacked numerous times before, and the whole ridiculousness of the situation is pretty frustrating because nobody opts in to Equifax. Nobody asked them to collect information on you, they just do it, and then they sell that information to their real customers, who are banks and credit card agencies, and we all know that 50% of credit reports, if not more, contain major errors that affect your life, and you have to go through all this rigmarole to go ahead and fix it. They collect the information without your permission. The information that they collect most of the time is bad and is rife with errors and then, they’re bad stewards of the information in that they leak every address you’ve ever lived at, your Social Security Number, your driver’s license number, your credit card numbers, and beyond all of that, they’ve got the nerve to offer you “protection” for the data that they’ve lost, so the people who took on the responsibility to collect all these information have the unmitigated gall to try to charge you to protect you for the information that they leaked without your permission. The whole system is fairly corrupt and bankrupt in my opinion.

Jacob Morgan: Yeah, no, it’s pretty crazy, but how does this happen, right? I think people are sort of familiar with what hacking means, but in the case of Equifax, I’m just curious, and it’s probably a naïve and silly question to ask, but I’m sure other people have it. A couple of people get together and they say, “Hey, let’s go hack Equifax.” They spend a couple of weeks trying to figure out a way in there or ... What does that actual process of hacking a company mean? Do you plan it out months in advance, do you-

Marc Goodman: What you're looking for me to do is to teach your audience how to become criminal hackers. Is that right?

Jacob Morgan: Yeah, why don't you teach us how to do this ourselves, man?

Marc Goodman: Right, so you can all end up in Federal prison.

Jacob Morgan: Exactly.

Marc Goodman: No, I think, to answer your question, each hack is unique and individual, but the one thing that we see increasingly is that cyber-attacks are automated. I guess this would be the third thing that is profoundly different from crimes in the past. In the old days, crimes were committed by human beings, right? Somebody had to take a gun or a knife and walk up to an old lady and try to steal her purse. Nowadays, that code can be written to actually carry out attacks. The overwhelming majority, 99% of cyber-attacks are automated. It means that there is software out there known as crime ware. There's software, and there's crime ware. There's actually software that can be programmed to commit crime, in the same way that you have software that will help you write a letter, like Microsoft Word, or edit a photo like Photoshop. There is software that will do denial of service attacks, that will do credit card fraud, that will do identity theft. Really good hackers have come together and written programs that attack, try to break into systems, and steal both data proprietary and otherwise.

A small percentage of those attacks are customized or bespoke, and those are often the high level attacks. When you think of state-sponsored attacks, Russia going after somebody's email, or the NSA trying to penetrate somebody's computer system, whether it'd be in Iran or North Korea, those are highly customized, but that's a very, very small percentage. Certain amounts of industrial espionage are highly customized, but most of it is automated, and the fact that it's automated is a huge benefit for criminals. If you think about Facebook, their entire onboarding process is entirely automated. You sign up. You put in your information. You upload your pictures, and all they have to do is host the code, which is why they can have nearly 1.5 billion members online. It scales their business model scales, and that's why their valuation is so high. Well, criminals have learned from that and the process of robbing one or two people at a time is highly inefficient, but creating a code that can rob a million people or a few hundred million, that is a business model that scales. We've seen the numbers of victims grow exponentially.

A few years ago, we had the Target hack and 100 million accounts were compromised there. We thought that number was ridiculously huge until we learned that Yahoo announced that they had 500 million accounts that were breached. Then, about a year or two, after the initial disclosure, Yahoo mentioned, "Oh, actually, it was a billion accounts that were hacked." Just about a month ago, Yahoo said the number was three billion. Now, due to the interconnected nature of the Internet, it's possible for person to reach out and rob three billion people. That has never been possible before in the history of humanity. The fundamental nature of crime is changing really rapidly.

Jacob Morgan: Let's look at the Yahoo example, three billion people, what if somebody will say, "So what? It's inevitable. Somebody is always going to steal my username and my password." Personally, my wife always says, "Aren't you worried that somebody is going to take your wallet and somebody is going to have access to your credit cards?" I'm like, "No, not really." I'm at a point now where it's more of an inconvenience than I'm worried about somebody stealing my credit card info because I'll just cancel it, Chase has their protection, so and so. I feel like a lot of people are assuming that the privacy and security doesn't exist anymore, it's like it’s inevitable, it will happen. If you look at something like Yahoo or Equifax, or Target, what's the big so what in there? Somebody has your username and password, or they know your address, what's happening with that information that is so harmful?

Marc Goodman: Well, a few things. First, I want to take on the issue of this being inevitable. I will go down fighting for both privacy and that people should not be hacked. That is something that I'm quite committed to. We can talk about that. I don't think it's inevitable that your house will be burglarized. I don't think it's inevitable that your car will be stolen, and yet, I don't know why we accept that it's inevitable that your accounts will be taken over or your personal information will leak. I think the fact that we surrender so easily to the process is part of the problem. The fact that people aren't outraged when this happens is surprising to me. Now, to your point, if you think about cybercrime as identity theft or credit card theft, yes. When Target gets hacked, that's 110 million credit cards that go out the door. With the Equifax, we had many millions of credit cards that went out the door. Yes, I understand that that happens. There's two types of attacks we have to talk about, ones that you can do something about and ones that you can't do something about.

There's a whole bunch of stuff that you can do to protect the data on your phone, and on your computer, and all the internet of things device that you have in your home, and we can talk about that. Then, there are other ways you become a victim of cybercrime through no fault of yours, because you shopped at Nordstrom's, or because you shopped at Target, or because you had a credit report at Equifax. Those types of things are harder to deal with, but what I want you and your audience to think about is that it's not just your credit card that is being hacked these days. There are so much information out there that leaks. Identity theft is actually much more serious than just having your credit card number replaced. We confound terms and we talk about, "Oh, yeah, I was a victim of identity theft. They took over my credit card." Actually, sustained identity theft where somebody goes out there and takes over not one of your credit cards, but all of your credit cards, and your Facebook account, and your credit profile, and starts taking loans in your names, and starts taking mortgages in your name.

That is really a very, very significant pain in the butt, and it could take you years, and years, and years to get back access to your own life. When somebody takes out loans in your name, or commits a credit card fraud in your name, those get reported to the police and warrants get issued, so you could be arrested because somebody else has misused your identity, somebody's been charged with forgery with your identity. That's one issue, but the data that's leaking nowadays, when somebody gets access to all of your Gmail accounts, and there's a lot of private information in there. Sometimes, people talk about really private stuff online, whether it'd be with their doctor, or with their psychologist, or with the person they're dating, or maybe they're married and they're dating somebody else. We saw some really interesting examples of private data leaking with the Ashley Madison hack. I'm not sure if you remember that case.

Jacob Morgan: I do, I do, of course.

Marc Goodman: Yeah, so there were 35 million people who paid to be a subscriber of Ashley Madison, and a whole bunch of really interesting stuff came out of that data breach. First of all, it was shocking to me that 35 million people paid to be part of that service, in case you-

Jacob Morgan: Can you let people know what Ashley Madison is, for those that aren't familiar?

Marc Goodman: Yeah, exactly. For those of you who don't routinely cheat on your spouses, Ashley Madison was a website whose motto was, "Life is short, have an affair." It was a dating service for people who were already married, and it offered them a way to cheat on their spouses. Obviously, that is something that most husbands or wives would not be thrilled with, if they found out that their partner was cheating on them, so the site offered discretion. Ultimately, they were hacked, and the names of those 35 million subscribers leaked. A bunch of really interesting things happened. First, criminal organizations got a hold of those list, and they started calling Ashley Madison subscribers, and they had your name, and your address, and your credit card, and they would call you up and say, "Hey, Joe, we've seen that you’re subscribed to Ashley Madison, and we looked on Facebook and we see that your wife's name is Kate, and we're going to call Kate and tell her that you've been cheating on her unless you want to pay this amount in extortion." A whole bunch of people were bribed and extorted based upon that. The other thing that we saw was that there were probably at least a half a dozen suicides that were traced back to Ashley Madison.

I believe a pastor somewhere in Canada killed himself. There was a police officer in Texas who committed suicide because they were so overcome with the shame of having cheated on their spouses. This is where private information is not just about your credit card number, but deep, deep personal secrets that people carry tremendous shames about, and led to actual death of human beings. For your audience, I want them to understand that cybercrime is not just about identity theft or credit cards. In this case, it was actually about people's lives, their deepest, darkest secrets. Your medical records could leak, and maybe you've got nothing in your medical record that you are worried about, but there are people out there that have had sexually transmitted diseases, that have HIV, that may be treated for all different types of disorders, that they want to keep private. Another way that we're seeing cybercrime manifest now is by hacking a video camera. You may think you've got nothing to hide but if you and your wife were in your bedroom, and there's a baby camera there, and some hacker is watching what you're doing, or is watching your wife breastfeed a child in the nursery through the baby camera, you definitely wouldn't want that information out there.

If you bring your cellphone into the bathroom, you probably don't want people spying on you through the camera on your cellphone. All of these things are other parts of cybercrime that the general public don't think about, and beyond that, there's something called critical infrastructure attacks, which can really cause havoc in societies. If you think about all the critical infrastructures of society, whether that be the electricity grid, the water grid, sewer grids, 911 systems, transportation systems, air traffic control, every single one of those systems relies upon a computer to work. There is no air traffic control without computers and radar of some sort. There is no electricity grid without computers to control all of that. Every single one of those computers is hackable, and we're starting to see criminals go after these systems. We even are seeing governments do that. The Russians took down the Ukrainian air traffic control system at the airport in Kiev during their spat between Ukraine and Russia. We've seen Iran hack into a dam, a water dam in Upstate New York and they were able to cause a flood in New York State as a result of releasing the dam water.

We've seen 911 systems attacked through DDOS and the like, distributed denial of service attacks. We need to think broadly about what a computer is. Your phone is a computer. The camera in your house is a computer. Your car is a computer. We're now entering the days of connected cars. Most cars built in the past 10 years have onboard computers that are hackable. We've now seen people do that, and of course, criminals are going to target self-driving cars as well.

Jacob Morgan: You're scaring me, Mark.

Marc Goodman: Good. Then, my plan worked. My goal is not to scare you though, it really is to educate you. Step one is to understand it's not just identity theft. We live in a connected society and the basic fabric of our society is hackable. Now, I want people to understand that technology is awesome, I’m not anti-technology. All these same technologies, whether it'd be social media, online learning, advances in medicine, they're going to have huge positive impacts on society. Talk about cars being hackable, yeah, that's going to be a problem, but we currently have 40,000 people a year that die in the United States alone due to traffic accidents, mostly caused by humans doing a terrible job driving, either when they're drunk, or they're texting, or not paying attention. We could potentially solve that problem and have 40,000 people survive that otherwise wouldn't, thanks to self-driving cars, assuming we can protect the technology. Technology is going to rapidly extend human life. It will reduce infant mortality and it can cure diseases that were never previously curable.

Technology is awesome, the only thing that I'm saying, and it's the message of my book, is that we need to take care. We need to protect these tools. Yes, we need to innovate, but we also need to think about the flip side of the technologies and begin to deal with that.

Jacob Morgan: In your book, you also had some pretty interesting examples of how terrorists were carrying out attacks on the ground based on data that they were getting online. Can you share maybe one or two of those examples as well? Because we've all been familiar, I think we're all familiar with a lot of the terrorist attacks that you've described, and a lot of the cyber hacking attacks that you've described, but we don't understand the other side of it, of how these things are happening, and how these people are actually using technology to make these things happen. We just see the attack getting carried out and say, "Oh, people burst into this building and they started shooting." But we don't have a context of, "Well, they actually figured all these out because they were using Google

Maps, they were using Twitter." Can you share some of those examples, because I thought they were scary, but very interesting?

Marc Goodman: Absolutely. People think of "terrorists" as being backwards people living in that country over there, that aren't very clever, and don't have much to live for, and that's why they're doing what they're doing. In some cases, that's true, but there are a lot of technologically sophisticated terrorists. If you go to the 9/11 attack, that was a pretty sophisticated attack. They had to learn how to fly jumbo jets, and take them over, and all of that stuff. There was a lot of technology behind that. If you go back, actually, to the first World Trade Center bombing in 1993, the one that most people have long forgotten about, that was carried out by a guy called Ramzi Yousef. He had a laptop computer, which back in 1993 was pretty rare. When the FBI identified and arrested him, they found that the data on his computer was fully encrypted. In a time when not many people were using computers, certainly not too many people were using laptops, and very few people were using encryption, you have the guy responsible for the first World Trade Center attack using encryption on his laptop to thwart the FBI, and in fact, it did.

It took years for the FBI working with the NSA to be able to decrypt that laptop and uncover evidence. If you go back to the 2008 terrorist attack on Mumbai, in India, which I think is the one you're referencing from my book, that was perhaps one of the most technologically sophisticated terrorist attacks of all time. The criminals there created immense advance research on their targets. They did look at Google Maps, they knew exactly where they were going. They understood how to get to each location because they had practiced it in their training camps back in Pakistan, and used Google Maps extensively. Technology was good for research. Technology was good, in that case, for fundraising, and technology was used, in that case, to actually kill more people. One of the thing that most people don't realize about the 100 or so people who lost their lives the day of the ... or the hundreds more that were injured, is that the terrorists did something very clever. They actually set up a war room back in Pakistan. If you've watched any television show, with the FBI in it, something like 24, you always see the big command center with the big television screens, and all the blinky things going on.

Guess what? Terrorists did that, too. The terrorists had set up their own war room back in Pakistan where they had people in direct touch with the terrorists on the ground back in Mumbai, who controlled them in real time. The terrorists operation center was watching BBC and CNN, and IBN, and all these other radio stations. As the news reports were saying things, "Oh, we think the terrorists are in Room 153 of the Taj Mahal Hotel, the terrorists’ war room was calling the terrorists on the ground, in real time and saying, "Hey, are you in Room 153?" "Yes, we are." "BBC is reporting it. Get out of there now. Is there a camera?" They were able to reposition their troops in real time as a result of the information coming out both from social media and from the legacy media. That allowed them to kill many, many more people.

Jacob Morgan: It's pretty scary. You had a great visual where you said the people had ... the terrorists had guns in one hand and cellphones in the other hand. I think that that phrase, I think, just speaks volumes for the kind of world that we're approaching. Most people probably had no idea that all these was happening, right? We just saw these attacks, myself included, I just thought that it was some crazy people that got some people together, stormed a building, and started shooting.

Marc Goodman: Well, in the preparations, again, going back to the cellphone in one hand and a gun in the other, on their Blackberries, they were actually, in real time, Googling people. At one point, they came across a guy in his room who they went ... The terrorists went from room to room trying to clear the hotel. They thought there was a guy in the room, they ended up shooting through the door, busted in there, and they found a guy who was obviously quite scared at the terrorist breaking into his room. He was hiding by his bed, and they saw him, and they asked him, "Hey, who are you and what are you doing here?" He says, "Oh, I'm nobody. I'm just an innocent school teacher." Well, the terrorist thought, "No Indian school teacher gets to stay in a top floor suite at the Taj Mahal Palace in Mumbai. They got his passport, which was on his bedside, and they phoned his name into the terrorists' op-center and those guys Googled him in real time, and they saw that he was one of the wealthiest man in India, I think the second wealthiest man in India who ran a bank there.

Once they got his name and knew who he was, they asked the terrorist war room, "Hey, what do you want us to do with this guy?" The war room said, "Kill him." A simple Google search nowadays can determine who shall live and who shall die. For people who are like, "Oh, social media, who cares? I'm going to share everything and it's all out there. Privacy be damned." This is a black swan case, a one in a million, I get it, but in this particular case, they were able to find this guy's profile online, and the fact that he was a bank president, and quite wealthy. Those types of things become possible.

Jacob Morgan: Yeah, even in my personal life, my wife was having this conversation with me the other day, and she's like, "There were some pictures of our child on Facebook." She's really concerned about that stuff. We've been watching Mind Hunter on Netflix which, I think, has traumatized her. We're seeing some of these shows on Netflix of these terrible people doing terrible things. Even in my personal life, we're thinking about, what information do we want on social? Do you want pictures of kids on social? How much stuff should we be sharing? It's definitely something that, at least, I'm thinking about internally here, which-

Marc Goodman: 93% of infants have a social media profile. It starts when mom posts the ultrasound photo, everybody puts the ultrasound-

Jacob Morgan: Yeah, exactly, which I think we did, too.

Marc Goodman: Yeah, right, so that all starts. The thing that will be different for your child, then, for you or for me, is that we had a portion of our life that wasn't lived online.

Now, from the minute you're born, with that ultrasound photo to all the toys that you're playing, all these "smart toys" are tracking children, of these children social networks by Disney and other are looking very closely, and you're able to build up a profile on a child, from the minute they're born until the day they die. It's kind of the DVR/VCR lifestyle, where you'll be able to go back and say, "Oh, yes, on June 3rd, 2021 I was doing this because I saw it on Facebook, or Tweeted this out, or posted this on Instagram." All of that data-

Jacob Morgan: Yes, [crosstalk 00:36:52] stuff.

Marc Goodman: Yeah, all of that data. The thing that people don't understand, if you think we live in the era of big data now, we're just beginning our journey into that world. All of these data can be crunched through machine learning and algorithms. Then, again, for people who think, "Oh, I've got nothing to hide." You get to predict things that maybe people don't want to be public. For example, MIT came up with an algorithm, which I think they called Gaydar, and it was a predictability score for somebody's sexual orientation, based upon whether or not they like Broadway plays, or whether or not their friends were openly gay, that they were linked to crazy stuff like that. There are other researchers that have come up with a socio-path or a psychopath score based upon the things that people will post, by being able to analyze their writings. Whether or not you're angry, whether or not you're a good employee, there are companies now, most people don't realize, that this was in other thing that I wrote about in my book, but we talked about the Ashley Madison profiles.

Lots of people have online dating profiles through match.com or OkCupid. I'll use OkCupid as an example because they were investigated by the Federal Trade Commission. You go ahead and you sign up, and then they ask you a bunch of questions that seem logical in the context of a dating profile, like, how many times a week do you have sex? Do you use drugs? Do you smoke marijuana? How many times a week are you drinking? Have you ever used cocaine? It may make sense if you would like using cocaine, and you're looking to date a girl or a guy that also really loves cocaine, OkCupid will help you make that match. It seems logical, but one of the things that people don't realize is the minute you say, "Yes, I drink seven times a week, heavily, and I use cocaine, and I have sex 42 times a week." OkCupid is dropping cookies on your hard drive, and literally, immediately, instantaneously, sharing all of that information with dozens, if not hundreds of third party data collectors who now know who you are because they've identified you through your profile, or through your credit card, or you logged in via Facebook.

Now, they know that you use drugs and you've admitted to using cocaine, and what they're doing is taking all of that data and selling it to third party companies, who are then selling it to employers, and even universities. When you go for that job at Google or Bank of America, who knows, I'm making those up, those are just examples. I don't know that they do this, but you go for a great job at an employer, and they do a background check on you. They're getting data from those third party companies, where you've admitted to use cocaine, and they're like, "You know what? Maybe we don't want you working at our company." You'll never know the reason that you are hired, but that's the reason.

Jacob Morgan: That's actually going to transition well into my next point, which is looking at how this impact to work, and maybe we can transition to that. Do you see any implications here for business, for the workplace, for employees, around either how companies are using data against employees. I know we've had stories about looking for insurance policies and stuff like that. I don't know if you are exploring that side of it as well, on the business, on the employee work side.

Marc Goodman: No, definitely. I do a lot of work with HR professionals, and heads of HR, chief human resources officers, and all of this is the story of the workplace. You asked me earlier, and I didn't fully answer your question about, how does hacking actually happen? I talked about the overwhelming majority of it being automated, but the one thing I didn't share is how it actually happens is people. According to IBM Security, 95% of all data breaches can be traced back to human error, that means that you got a link on Facebook, or on Facebook Messenger, or a text message on your cellphone, or an email in your inbox that looked interesting and you clicked on it, whether it was, see Justin Bieber naked, or see Miley Cyrus naked, or here's today's lotto numbers, whatever it is. Criminals are really good at psychologically exploiting you and getting you to click on stuff, and so, 95% of data breaches can be traced back to human errors. In the workplace, that's a huge problem for companies because if your employees are not aware of this risk, they're putting your firm at risk.

If you go back to the Equifax hack, the way that that happened is, one of their employees charged with updating the software on one of their web servers didn't do it. Human error led to the leak of a 150 million credit reports, thank you very much. If you have a company and you have employees, and those employees are human, that 95% human error thing should be of concern to you. It's a great opportunity for you to train your employees on how to not just protect your company, because frankly, if they are driving a Coca-Cola truck, delivering bottles of Coca-Cola, they don't think too much about protecting the corporate network. Everybody thinks, "Oh, the IT department will do that, or the Chief Security Officer will do that." The bottom line is, your employees are being hit everyday with malware and bad links, and denial of service attacks, and ransom ware. Educating them can be a huge impact to the company. I think most company should clearly have a way of training employees. We're starting to see companies do what are called fake phishing attacks. There are companies that will send out emails to their employees and see if they click on them.

If you click on an email that is a phishing email, you will be spoken to by your boss, and the second time you may be spoken to by your third boss. There are some companies that have a three-strike and you're out policy. If you click on a dumb link three times in a row, you're going to find yourself fired. That's clearly an issue for companies, is protecting their information. The other thing that, surprisingly, most people don't realize is that cyber bullying just doesn't happen to teenagers. If you said cyber bullying, you might think of a mean 12-year old girl, or a group of mean 12-year old boys and girls, harassing one of their classmates. It turns out that nearly 50% of employees have experienced some sort of cyber harassment in the workplace at the hands of their other employees. This creates a huge nightmare.

Jacob Morgan: It's not anonymous, they know who these other people are.

Marc Goodman: Well, sometimes it's anonymous, and sometimes, they know who they are. It's a little bit of both, but frequently, they know who they are, because people will post things online in their real name, shockingly. Some of that can fall into the category of sexual harassment or gender discrimination, or discrimination based upon race, or sexual orientation, or religion. All of that stuff is an issue that the employer needs to be aware of, because they can easily be held liable for the action of their employees, particularly if it's brought to their attention, and they don't stop it. Workplace cyber harassment and cyber bullying is a really big issue, and it's growing. Companies need to have policies around that, there needs to be education, and of course, zero tolerance for these types of issues. We all have issues around technology in our lives, and what happens in our personal life affects our employment. If you, God forbid, have got a kid who has cancer, or you're going through a divorce, or your wife or husband is an alcoholic, obviously, you bring those issues, those life issues to work, and they become work issues. The same is true with things like identity theft. I talked about how many years that can take to fix that problem.

If you have employees who are a victim of identity theft or cyber bullying, that's going to impact the workplace, too. There's a huge opportunity as an employer to educate your employees on this issue, and we're starting to see employers do that. Employers are offering, increasingly, a workplace fitness programs, because they realize people who are in better shape cost less money to the company's healthcare plan, and they're better more effective employees. We see companies that offer free financial counseling for their employees around retirement, and other issues that they'll be taken care of. I think it's high time that employers help their employees start to navigate some of these technological risks so that they'll be happier and healthier in their own lives, and ultimately, that will also protect the company.

Jacob Morgan: Yeah, no, those are all very good ideas. I've had my own fair share of people creating fake Twitter accounts about me, and leading all sorts of angry comments on LinkedIn, on Twitter, on Facebook. Just like a group of people are [inaudible 00:45:59] me around the web, that I've pretty much just ignore. I think it's a very, very common thing. I'm sure you probably have this. There are some people out there that say, "Oh my God, Marc is an idiot. He doesn't know what he's talking about. He's terrible."

Marc Goodman: Only people who know me well say that, never the first day. Yeah, obviously, it's something that we have to deal with, and you've seen companies like Facebook and Twitter come under increasing scrutiny for allowing that, because frankly, the methods to report abuse have been really, really weak up until this point. We need to fix that, and more and more States are jumping in. I forget the statistic, it's in my book, but it was something shocking like, 40% of 5th Graders had seriously considered suicide as a result of cyber bullying. These are little itty bitty kids who are being driven to seriously consider suicide as a result of cyber bullying. I forget the exact statistic, but it was something like that. It's in the book.

Jacob Morgan: Yeah, it's completely out of control.

Marc Goodman: Right, and we're seeing that play now. Of course, that goes from the school, to the workplace, to politics, to our country, we're seeing that. People who think that they can launch these anonymous attacks become embolden, and it really plays out in a way that's detrimental to society, and again, when we talk about cybercrime, this is a great example of something that's not just ... "Why should I care about cybercrime? It's just my credit card." Well, when your personal data leaks, that's something that people can use against you. I had mentioned earlier about hacking cameras. There's a really telling story of Miss Cassidy Wolf who was Miss Teen America, 16-year old girl, obviously beautiful. One day, she was sitting at her home computer and she gets an email message. The email message basically said, "You better have sex with me or I'm going to release these pictures." She looked, and there were a dozen pictures of her naked in her own bedroom, that this person was threatening to post on Facebook and release. It turns out, she had a laptop in her bedroom, like most students do. When she came out of her bathroom, toweled off after the shower, somebody had hacked her laptop and they were able to take control of her camera.

As a result of that, they were now extorting her to have sex. Fortunately, she told her mom, who then told the police, who then told the FBI, and they investigated it. They were able to trace it back to one of her classmates, but there are other stories were young people were coaxed by what they thought were other young people into sexting or showing one of their breast, or their private parts, somehow. Then, they became a victim or extortion, often at the hands of pedophiles, much older than themselves, halfway around the world. We've had many, many suicides. There was a very famous case of a girl up in Canada, 13 years old, who had a picture of her topless posted online. Then, of course, her classmates teased her. She ended up committing suicide as a result of it. Again, it's not just about credit card theft, this data, this information, this bullying not only can affect your personal life, but us as a society as well.

Jacob Morgan: It's funny because you don't ... Well, not funny, scary, because you don't even know when this happens to you. You don't really know what information hackers have about you or if your information gets leaked in certain things. I know Equifax, they had something where you could type in your Social Security Number, and they give you, "We don't think you've been hacked. We don't think you've been affected." By and large, when a company like Target gets hacked, or any other company, you really have no idea if you’re implicated in that or not. How do you know as an individual how safe or protected you are?

Marc Goodman: I'll tell you. There's a few things that you can do and as we wind down our chat, maybe that's a great area to focus in. First, I'll say, a lot of this comes down to law, public policy, and regulation. I'm not a guy who likes to create regulations. I think the government's broadly not the most effective way to handle a lot of problems. That's a very broad brush, but I think here's an area where regulation could potentially be useful, and I'll give you an example. California was one of the first states to have mandatory data breach notification. If your data was leaked, whether it'd be through the Anthem Blue Cross hack, or dozens [inaudible 00:50:43] hack, you needed to go ahead and notify everybody who was a victim. What was happening is, banks, and I think there was an example, Citibank, I believe it was Citibank, but don't quote me on this, had a big data breach, and maybe it was J.P Morgan Chase, which definitely did have a data breach. As a result of the California Law, everybody in California was officially notified, "Hey, your banking information was hacked and et cetera, et cetera, and we just needed to notify you about it."

People in the other 49 states were not notified, because there was no law mandating it. Eventually, that leaked that the bank did not tell all the people in the other 49 states, and then they did, but the only reason why they did is because they were shamed into it. Really good data breach notification laws are important, and I think there needs to be really strong penalties, because the fact of the matter is, companies are going to leak your data as long as it doesn't really cost them. Now, I saw a statistic that said the Equifax data breach might end up costing $70 billion, that one leak was a $70 billion event. We're going to see more and more companies go bankrupt as a result of this, but I think that we need to make the companies pay, because if they're not paying, then, they're not taking the problem seriously. We see, for example, if you try to open up a bank account now, they ask you for all different types of identification, because the banking industry has been taken to court by the Federal government for money laundering, so now they take that seriously.

We need to get all companies, whether it'd be healthcare companies, insurance companies, social media companies, to be held to account for that. If you want to know if you've been hacked, there are two websites that people can go check out. One is called Have I Been Pwned, P-W-N-E-D, and that’s hacker talk, pwned kind of comes from owned. If somebody owns you, it means they've taken over your account. Have I Been Pwned, P-W-N-E-D, Google that, and you can put in your email address, and it will show you all the different data breaches that you had been inculcated in, because they gather data from the dark web. The New York Times also has a really cool feature showing Have I Been Hacked, and they'll ask you, do you have an account on LinkedIn, did you ever have health insurance through Anthem Blue Cross, and then, they'll show you that as well. I think the best way to deal with this is to know how to protect yourself, and if you'd like I'm happy to talk about some things that people can do to protect themselves.

Jacob Morgan: Yeah, please. Well, maybe, really quick, let me transition to the business thing, and then, we'll wrap up on that, because I think that's a great way to end. I had a few CIOs that were on the podcast from companies like GE, from IBM, and they all told me that they get thousands of people, or not thousands of people, thousands of hacks a day that try to ... potential hacks of just things that are trying to break into their systems, which is completely amazing, when you think about it, that thousands of times a day, something is trying to break into your system. It's just mind-boggling.

Marc Goodman: That's the automated factor that I was mentioning.

Jacob Morgan: Exactly.

Marc Goodman: Don't think of that as people sitting at keyboards, that is just automated software, literally tens of thousands of times a day trying to break in a big corporate network like GE or Cisco.

Jacob Morgan: What advice do you have for business leaders at organizations that are very concerned with privacy and security? One of the things that I've heard is that a lot of business leaders are accepting that they can't protect everything, so they just focus on protecting the core things inside the company, and everything else, they put security around, but they acknowledge that they can't protect it. Is that the right approach for this, or what do you recommend?

Marc Goodman: Well, I think that is a good approach. It is one that's increasingly common. The old method of cyber security was, "We're going to put up a firewall and we're going to keep everybody out." Those days are long behind us. The bad guys are in your network right now if you are a company, and you need to hunt them down, and find them. In the same way that the government classifies information, top secret, secret, confidential, unclassified, et cetera, they recognize that we can't protect everything. We're going to work really hard to protect the top secret compared to the confidential or unclassified, and yes, you need to do the same inside your corporation. As to other things that company leaders can do, whether it'd be CEOs, CIOs, or heads of human resources, I strongly, strongly believe that you have an imperative to educate your workforce on the risk and teach people not just how to protect the company, but how to protect themselves. The other thing that you need to do is start thinking exponentially, which we haven't even discussed yet, but the point is, the threat is accelerating much, much more rapidly than you realize due to Moore’s law and many, many other factors.

You don't need to be thinking about what the problem is going to be tomorrow, you need to be thinking about what it's going to be the day after, and the month after, and the like. As Wayne Gretzky said, "Skate where the puck is going and [inaudible 00:55:51] for that." All of this comes down to creating a culture of cyber security. You asked me earlier how I spend my days. I spend big chunks of my time with corporate C-Suite and boards of directors helping them build a culture of cyber security, and that's a big part of my consulting work.

Jacob Morgan: Which is very important. We definitely need more people like that are out there. All right, so what about for individuals? Whether they're employees or not, do you have any advice for what individuals can be doing to better protect themselves in this new world?

Marc Goodman: Absolutely, first, I'll say, because there's a lot of information out there, if you go to my website, futurecrimes.com and click on tips, so just go to futurecrimes.com and click on tips, there's a whole bunch of information there on what you can do to protect yourself. I've created an infographic. The good news is, and this is why I wanted to end the podcast on this note is that these all sounds really scary. It all sounds like there's nothing that you can do. It turns out that small steps make a big difference. Having a heart attack or getting cancer sounds really bad, but if you learn that, "Well, actually, if I don't eat too much and I exercise a lot, and don't drink, and do certain things, I can actually significantly reduce my risk." You don't have to be crazy about it, just small steps make a big difference. The same is definitely true with cyber security. The infographic, with all of these tips that I mentioned, is based upon research from the Australian Ministry of Defense, who studied hundreds of thousands of cyber-attacks. They discovered that if you basically took six steps, you can reduce your cyber risk by 85%.

These things involve being very careful about what you click on, most importantly, updating your software, the software on your router, the software on your phone, the software on your computer. That alone is a massive, massive drop in your ability to become, or becoming a cyber-victim, just updating your software, because companies are constantly identifying those viruses and bits of malware that are out there. If your software isn't up-to-date, then once those viruses or vulnerabilities in, for example, Microsoft Office or Microsoft Windows is out there, then, criminals are taking advantage of that, and they're building new attacks to go after it. Most important, update your software. There's lots of good advice on the infographic about passwords. One thing to keep in mind, 70% of people use the same password across multiple sites, 50% of passwords are over five years old. The problem with that is, if your information leaks in Target, your Target account leaks, or your Yahoo account leaks, the very first thing that criminals are going to do is take your Yahoo sign on and password.

I talked about automated tools, they're then going to try the same exact credentials against Facebook, against LinkedIn, against Bank of America, Wells Fargo, your health insurance company, and most of the time, it's going to work. You should have a separate log-on for every single one of your accounts, which is daunting, because now, the average American has over 100 online accounts. Everything from your kid's school, to your health insurance company, to all your social dating networks, et cetera. I recommend a tool called a password manager or a password wallet. There are several reputable companies out there like Dashlane or 1Password, they will manage all of your passwords for you automatically, and thus far, have done a good job of doing that. They also have really cool features, so that let's say you did have a Yahoo account stored there, the minute the Yahoo breach becomes public, these password managers will tell you, "Hey, there's been a breach at Yahoo. Would you like to change your password?" They'll do it automatically. I'm a big fan of those tools.

I'll give you one other, which is a bit more technical, but is super helpful, particularly for people on Windows, but it also works for Mac. Most people only have one account on their computer. If you log on to your laptop, you log in with just your name. I don't know, do you have one account on your computer or multiple?

Jacob Morgan: I have one account on my computer.

Marc Goodman: Right, are you on Windows or Mac?

Jacob Morgan: I'm on a Mac.

Marc Goodman: Okay, so what that means is, by default, your account is known as an administrator account. An administrator account has full privileges to change anything they want on your system, and you need administrator access, for example, if you want to update your software or change some of the core files. We all need, at some point, administrator access. The problem with being logged in as administrator, however, is that if you click on a bad link, or somebody sends you an infected PDF, or you go to a website that's got bad Flashcode in it, because you're the administrator, that virus can automatically execute and make those malicious changes to your system. That's how you get infected, and that's how you get owned. I tell people, you should never, ever, ever surf the Internet or do the majority of your work from an administrator account. You should create a second user account, and therefore, do all your work, your banking, your shopping, your surfing on that user account. Let's say you go to click a link that's supposed to be a YouTube video, if you're doing that on a user account, in order for that malicious YouTube link to infect your computer, it's going to need administrative access to your device.

If you click on a PDF file or a YouTube link and you'll get a pop-up that says, "Please enter your admin password." You should know, "I don't need an admin password to watch a YouTube video." That's a clue that somebody is trying to hack you. What's fascinating is, Microsoft did a study on using admin accounts and they said, "If people didn't use admin accounts and only used a user account, they could avoid something like 90% of all attacks against the Microsoft operating system, something like 97% of all attacks against Microsoft Office, and 100% of attacks against Microsoft Explorer or Edge. Just that one change alone can drastically reduce your risk in the world of cyber risk.

Jacob Morgan: Yeah, that's amazing. Well, it's funny, we didn't even get a chance to talk about 3D printing, the Internet of things, DNA hacking, we touched on AI a little bit, but you talked about all sorts of really cool stuff in your book. Where can people go to learn more about you, your book, if they have any questions, I know you mentioned your website, but maybe you can just let people know how to connect with you.

Marc Goodman: Sure. Well, you can follow me on Twitter, @FutureCrimes, that's where I'm putting out a lot of these latest threats and tips for people to protect themselves. I'm @FutureCrimes on Twitter, futurecrimes.com is the book, and there's some info there. If you also go to marcgoodman.com, Marc with a C, you'll see all the latest info that I'm polling together on this topic, stuff that I've written, whether it'd be news articles and the like. You can also reach out to me on the website. If people have particular questions, there's a whole FAQ there. I often get questions from people who want to, for example, learn how to protect themselves, or maybe they're interested in a career in cyber security for themselves or their kids. They want to know what they can do to protect themselves or their business. You can reach out to me with any and all of those types of questions there.

Jacob Morgan: Just so I make sure I understand, you're an optimist when it comes to the future of this. You're not a skeptical pessimist who believes that there's no such thing as privacy and security, and that we should just lock our doors, and bolt them shut, and disconnect everything from the Web?

Marc Goodman: Absolutely not. Believe it or not, I am what I call the irrational optimist, because in my work in law enforcement and counter-terrorism, and national security, I've seen lots of bad stuff out there, but the bottom line is, there are still way more good people out there than there are bad people. The good people vastly outnumber the bad. If you look at some of the worst things that have happened, whether it was the 9/11 incident, or the shooting in Las Vegas, the shooting, or the terrorist attack gets the headline, but what was amazing is that people, thousands of people came together to help out victims of the shooting, victims of 9/11. Overall, I absolutely believe that people are good at heart, and vastly outnumber the bad. When it comes to technology, these tools, as I said, are going to radically extend human life, cure diseases, educate the masses, bring billions of people out of poverty. It's going to be a really exciting time for humanity, but there are risks, and all I'm suggesting is that we address the risk now.

We're about to enter the age of the Internet of things. In fact, it's already started. We're going to add 50 billion new devices to the Internet by 2020 according to Cisco. Now is the time to lock down and secure those devices, because once they're online and hackable, it will be too late. We have some work to do as a society. We have work to do as citizens. We have work to do as business owners, and as employees, and as parents, but the work can be done. If we take those small steps, it can make a huge difference, and that's why I remain optimistic.

Jacob Morgan: Well, I love it. I think that's a great note to end on. Marc, thank you very much for taking time out of your super crazy busy schedule to speak with me.

Marc Goodman: Thank you, Jacob, the pleasure was mine.

Jacob Morgan: Thanks, everyone, for tuning into this week's episode of the podcast. My guest, again, has been Marc Goodman, make sure to check out his book Future Crimes: Inside the Digital Underground and the Battle for our Connected World. I'll see all of you guys next week. Hey, everyone, it's Jacob. If you're interested in the Future of Work and want more content around the latest trends, ideas, strategies, and stories, then make sure to visit thefutureorganization.com. Here, you will find all the podcast episodes, articles, research and my YouTube series, where I explore the future of work in short two to three minutes snippets which are all professionally shot and edited. If you want to join the newsletter, you can text the word FUTURE to the number 44222, or visit my site and sign up there, that's thefutureorganization.com. Thanks again for tuning in, and remember to rate the podcast on iTunes or wherever else you are listening. I will see you next week.