Bill Murphy: Okay, Mark, I want to welcome you to the show today. We are live.

Mark Sangster: [crosstalk 00:00:09].

Bill Murphy: We're almost live.

Mark Sangster: Almost live. Pleasure to be here.

Bill Murphy: So, this has been great. I have read your book here, I love it, No Safe Harbor: The Inside Truth About Cybercrime - and How To Protect Your Business. But before we jump into the book, let's talk about you and kind of your origin story. Tell me a little about the trajectory [00:00:30] of how you got started in technology as far back as you'd like, whether it's high school, grade school, college, whatever it may be. And then, let's bring it up to the book, and sort of the origins of the book and the stories that you tell within it.

Mark Sangster: Yeah, absolutely. So, I think of way back in the day, as a kid, I had delusions of being a pilot, and that didn't work out for various reasons. And I ended up sort of, I guess walking backwards into... As they say, the road you take to avoid your fate is the one you meet [00:01:00] it on. And I ended up in technology, and I started out early days, I worked for companies like Cisco, been with BlackBerry way back when it was called RIM, Research In Motion, and I worked on the first security, or their very secure devices that they were building for the government at the time, which were kind of fun. Because you would encrypt, but you would send an email, go get a coffee, maybe get lunch, to check to see whether that had actually gone, back in the day, right?

And then, from there, I kind of kept moving through, [00:01:30] worked for Intel, ended up... I joined a company called eSentire, which at the time was a small security firm. And the thing that really I found most interesting about that, was that the basic clients they had, they weren't the big banks, they weren't the big insurance companies, they were these small, mid-sized financial institutions, and some law firms, and some healthcare institutions, and these were the ones that were the most vulnerable.

And I ended up spending a lot of time trying to translate the security risks into [00:02:00] a sort of more common non-practitioner language that other people in the business... The business side of it, the executives, the management, and so on, who didn't understand the technical risks, and often just saw it as, it's hyperbole, or you're selling fear, and sort of bringing them to terms with it in more of a sense of risk than as a sense of, as I say, an IT budget to manage, or unnecessary evil, as we've all heard during our time.

And there was lots of stories [00:02:30] that developed doing that, a lot of clients that we worked with where we saw very interesting, sophisticated, and elegant types of attacks and schemes. And what I really saw was... I could keep talking in boardrooms over and over and over expressing these risks and these issues, and while that was effective, it was very localized. I really started to get to a point of like, well, how do I find a voice for a platform that I can start talking about this more broadly? Because I feel like we all, or many companies suffer in silence, right? They [00:03:00] are a target, they have something worth stealing, and unfortunately, they don't realize that they and their peers are being hunted by criminal organizations.

Bill Murphy: I mean, I'm, as you know, in the IT security business, and I've working with CIOs for 25 years... Looking at the board, 51 CIOs coming to our next innovation forum, and I talk about innovating with defense and innovating with offense. And so, [00:03:30] of course, everybody wants to talk about the offense, and that's fine. We'll talk about the offense because that's fun. But the defense requires innovation as well, and new thinking. And I think the risk especially for the mid-market CIO is, I love your approach, because it is 100% needed to talk about security from a risk point of view. And I know that's one of the big theses of your book, right?

Mark Sangster: Yeah, no, absolutely, right? That cybersecurity is not [00:04:00] an IT problem to solve, or to fix, or manage, it's a business risk to manage, right? And you need to think about business outcomes, as they say, not sort of the technicalities of whether or not my firewall is configured properly, or I've misconfigured something in my cloud security settings.

Bill Murphy: So, how did you come up with the name, No Safe Harbor?

Mark Sangster: Ah, lots and lots of debate, right? I mean, I think I started out with things far more drastic like lessons in disaster, and [00:04:30] I had taken very much... Since there are some stories in there from aviation, and mining, and energy, and so on. I was taking more of that kind of approach working through the publishers, they're like, "Well, perhaps we could tone it down a bit." And maybe it's also a little bit of a play on the whole concept of... The sort of the safe harbor legislation, or privacy legislation that was at one point, which of course has been struck down. That's why we kind of went to that.

But it's also why the second part of that title is, The Inside Story to Cybercrime - and How To Protect Your Business, [00:05:00] because I wanted to be very clear that this is the point, is that, we want to talk about the stories and build them into our conversation so that we understand how they work, why criminals are motivated... Or I should say, how they're motivated, how they go about doing what they do, and what the implications are and the risks for the business, so that we can give them a clear line of sight to protecting themselves.

Bill Murphy: Yeah, I think the way you did the storytelling really talks about... [00:05:30] I think people know that, okay, we've got ransomware, but they really don't really understand what's behind it, and the motivating forces around it. We understand the global drug trade, we understand that we got to grow things, and so I love this concept of metaphors and analogies, because there's largely of this invisible digital ones and zeros universe in a computer that we're peering into, these browsers. And the browsers can be for the dark web, or for, [00:06:00] I guess, the non-dark web.

And [inaudible 00:06:02] we don't really have analogies for security risk associated with that, and maybe that's a good starting point for us right here. What's the one story that you find most often surprises you that people don't understand about the... I'm going to call them, the dark forces, but basically, [00:06:30] the underlying mechanics of the digital bad actors?

Mark Sangster: Yeah. You used ransomware, and maybe I can start there, is that I think people see this as a very sort of opportunistic, transactional, and self-evidently fake type of attack, right? I get an email from my banking service and the logo misspells the name, as a simple example. So, we sort of lull ourselves in this false sense of security, well, I can detect that, I'm not going to fall for that. The reality is, that's [00:07:00] not what they're targeting you with, right? They are socially engineering your company; they're looking at publicly available information. They're doing what I call cultural engineering, which is, determining who key players are, influencers, regulators, governing bodies, and so on, that they can then mimic as a way of creating an automated trust relationship, right?

When they start to understand that it's a little more creepy than they thought it was, right? That they've done a lot to understand who their victim is before targeting them, that they're invested, that [00:07:30] they use Fortune 500 types of approaches, right? Just so that... The MBA approach we use, right? So, they resell ransomware, they work as a gang. What if it turns out they have a great way of delivering malware? Well, you can hire that transportation company or gang to mule your malware, and then you get somebody else who's got a really effective ransomware set. So, you're hiring them for their toolkit to deploy and so on.

Why are they doing this? They're doing [00:08:00] it to reduce time to market, reduce their operational costs. And because it's of a high efficacy, there's a likelihood of more revenue, right? So, increase revenue, decrease costs, its profit by any businessperson's definition. And when they start to understand that they look and smell and think just like you do, that's where I think execs sort of wake up, because they realize like, "Oh, hang on, I am playing this game of chess, and I'm playing against a well-armed, well-funded, and highly [00:08:30] talented adversary."

Bill Murphy: I've explained this before, are you finding through your research, it's largely decoupled? So, there's not one organization but it can be... Someone is creating the malware, and then someone distributes the malware, and someone has access to the email, someone has access to... So, there's different [inaudible 00:08:56] largely a combination of [inaudible 00:08:58] decoupled organizations.

Mark Sangster: [00:09:00] Yeah, yeah, so there are. So, you definitely have the state sponsored actors that are clearly funded by a government, right? Whether they work directly for it, or they're just somehow indirectly funded. And there are organized criminal cartels. Yes, it's the ecosystem, I think is the most revealing piece of this, is that they work just like other businesses do. If you've got a good tool for tracking my customers, or delivering my email messages, or whatever it might be, I'm just going to hire you because I don't have to solve that problem.

So, understanding [00:09:30] that they work with these sorts of coupled approaches of picking best in class, all the kind of terms we would use, they do the same thing, that there is effectively, a self-sustaining economy for that kind of criminal activity that we can measure in terms of supply and demand, just the way that we would, whether we make widgets, or we provide healthcare or legal services.

Bill Murphy: I found it interesting just to know kind of the growth, even being in the industry, just [00:10:00] more in the blocking and tackling aspects of it. It was interesting you talking about... I think since 2017, it's a $6 trillion industry right now, cybercrime, but had doubled in the past three or five years. Is that what you said?

Mark Sangster: Yeah, no, absolutely, right? So, we're beginning to see this sort of almost exponential growth when it comes to sort of the profits and the revenue. And in fact, even more recently, in my role, particularly with the company, with eSentire, [00:10:30] we see the stuff, we see the threats and the attacks at the front end of the funnel that we stop. But the back end of the funnel, or the things like insurance claims... There's lots of insurance reports, even for 2020, that show the first half of the year doubling in ransomware and fake invoice, or fraudulent wire transfer attacks, 150%, I think, increase in the ransoms themselves. And it's really more than that, because five years ago, they were asking for the equivalent of $500. Now, they're asking for 5 million [00:11:00] or even 50 in some cases, 50 million, right?

So, we're seeing that, and we're seeing business email fraud. So, the fake invoices or the fraudulent wire transfers, that's gone up, but that's, again, doubled just since the first half of the year. Some of that, you can probably blame on COVID like many other things, but there's criminal efficiency here. As I said, there's a very strong economic engine, which means, whenever [00:11:30] there's gold in the hills, then everyone wants to prospect and strike a claim, and that's exactly what the criminals are doing.

Bill Murphy: A couple of things that I think people sometimes always come, and they go, "Why aren't people backing up their system, so they don't have to worry about whether their systems are ransomed? Are encrypted and unaccessible?" What is your response when people ask you that?

Mark Sangster: So, I think there's a couple of things there. Some companies just simply don't. But there's a lot [00:12:00] of companies that do what I call... It's they run the traffic lights with their eyes closed, and they hope for the best. So, they take out some form of insurance, right? They have a policy, and they get some kind of backups, and that's it. They lull themselves into that false sense of security. And what they don't understand is, yeah, maybe back in the easy days, that you're right, they would... A bad guy would come along and encrypt a laptop and say, "Give me $500, and if you don't..." Well, get your family pictures and your tax returns back. Nowadays, they're looking for millions because they've sown ransomware [00:12:30] throughout your organization, including backups if they haven't been properly, air gaped.

And then, they detonate. In a coordinated effort, they're looking or seeking a massive operational disruption, so whether they take down a factory, or a hospital, or a bank, and now that they know you can't conduct business anymore, now they're negotiating a ransom. So, we're not talking $500, we're talking 500,000 or 5 million, or in some cases, even we've seen... I think 46 billion was the biggest one I've seen. So, it's a lot harder to eradicate, and it's not as simple [00:13:00] as, well, I have backups and I bought some cyber insurance, so I'm good to go.

Bill Murphy: In a mid-market, which you and I were just talking about, small to mid-market, I find often the CIO... Literally, they're trying to be strategic, they're trying to be... But that many of them have grown up through the tactical ranks, so they certainly understand everything that's happening technically, most of them. But they're also being asked by the business to help invent the future, they're working with the business to bring revenue and play offense. [00:13:30] And so, they often delegate that backup, and they're not asking their teams to actually prove and verify and being very rigorous about the approach. And quite honestly, often, is the general going down into the troops and saying, "Is everybody fed? Are we actually making sure everybody's clothed?"

They're making some assumptions that we're going to clothe the troops, right? And we're going to make sure that the troops are healthy and well, but [00:14:00] it's an easy thing to... And then, you talk about this concept of wolves at the door, I thought that was great, chaos, invisible gates, and then wolves at the door. And the wolves at the door was this increasing complexity, is we're not just backing up systems on-prem, but we've got colocation facilities, and then we've got AWS, and Azure, and we've got a... Essentially, how do we approach this very much more complicated world?

Mark Sangster: Yeah. So, you’re kind of hitting on a couple of things here, the first is that we actually introduce as a business much of the risk. [00:14:30] Yeah, we can talk about sophisticated threat actors and nation states, and all kinds of stuff. Well, they're part of the equation. But the other piece of this is the things that we bring in.

Bill Murphy: [crosstalk 00:14:40].

Mark Sangster: So, like this emerging technology, moving confidential, protected information to the cloud, right? IoT and industrial IoT connected systems. So, we see business gain from them, there are business advantages, the business decides to do that, right? Like a law firm says, "Well, I want our E-discovery and dock management systems to be in the cloud, because it's [00:15:00] cheaper and more effective. Healthcare is connecting patients [inaudible 00:15:03], manufacturing can be done remotely and tied into ERP systems to streamline operations. So, we do these things because we see the business benefit, and then it's almost this afterthought where we go, "Well, heck, hang on a second, we probably should get the security guys in here to take a look."

Bill Murphy: [crosstalk 00:15:17].

Mark Sangster: But the ink is already dry in the contract, and that is certainly one of the biggest issues. I think the other thing with that is that we don't think of this as an evolving landscape. So, we still [00:15:30] have a bit of a set and forget mentality. Well, we just deployed this cloud system, well, we've got it secured, we got backups, we're good to go. But it constantly changes. And the examples I give here, I start or I end with COVID-19, but I can go back. Post 9/11, our concepts of disaster recovery and business continuity were predicated on full on premises protection, right? Okay, let's hopefully not talk about something as tragic. But there's a fire or a flood in the building, and the power goes out, so how do we continue to operate?

[00:16:00] So, we moved our backups across the river into Hoboken, New Jersey. And then, over a decade later, Hurricane Sandy rolls up the coast and floods Lower Manhattan and floods New Jersey, it doesn't care about state lines, and it can get across the Hudson. And then, we suddenly realized, well, you know what? That wasn't good enough, we now need to be colocated and have live backup systems that can take the load of our business, and we need to do that across the country, or in another domicile, and there's all sorts of legal issues with that.

And then, of course, COVID runs along, I think that's the third stool [00:16:30] on the virtual reality leg, I call it, because now you have remote workers with distributed remote workloads managing assets in the cloud. And it's like, well, there is no premises anymore. That means it constantly changes. So, what you did today... What got you here, won't necessarily get you there.

Bill Murphy: Yeah. Security is definitely moved. It's funny back in the DR, the Disaster Recovery days, and I've been in this world working with credit unions, putting these [00:17:00] early DR sites, and then it was cold, cold, or hot, cold, and then it was hot, warm, and now it's always on. It always is the better decision to have it always on.

Mark Sangster: That's right. That's right.

Bill Murphy: But now, the security is... A CIO recently told me... Actually, CSO said, "I used to have 35 offices that I had to protect 700 users, and now we got a firewall, 700 users, and [00:17:30] that's an exponential problem, that's way over 10X problem to have. And not only the digital part, but then they've got... As you know, with these... Having compliance for a financial services organization, they can't just print-

Mark Sangster: Absolutely.

Bill Murphy: You can't just print documents out and leave them in your little study off the corner of your bedroom.

Mark Sangster: That's right.

Bill Murphy: So, it's an interesting challenge we have [00:18:00] right now.

Mark Sangster: Yeah, you know what? Remote workers has... I think there's a few things that have happened. One, obviously, is the downdrafting of security to consumer grade tech, right? So, I probably spent the first few... March through June helping organizations make sure that their employees, their ISP's router, whoever you get that from, didn't have the default administrative passwords on them that you can just simply google, that they had encrypted their WiFi, that they weren't using their surname, or [00:18:30] their address as their WiFi name or SSID. And I kind of kidded that we had moved from BYOD, was bring your own device, that we're now BYOH, which is bring your office home. And it changed both the technical hurdles that we had to deal with, like I said, simple things like addressing security on an internet gateway at home.

But the other piece of that was the downdrafting of security awareness to the employee, now you have... It's not as simple as an [00:19:00] IT person using a remote administrative tool and logging into their laptop and changing some settings. You're not sending everybody out to your home. Even like as we're doing now, I had to work with people who in their Zoom backgrounds had confidential information, like financial records and account info on a whiteboard, you're like, "Buddy, you got to take that down." Or, if you're an exec, how do you destroy physical documents? Say, you print out financial confidential reports, I mean, you can't just chuck them in your trashcan. [inaudible 00:19:29] [00:19:30] Someone is not dumpster diving right outside your house, but there's a risk there. What happens if that gets [inaudible 00:19:36] and somebody finds healthcare records and patient records, and these kind of things have happened.

Bill Murphy: One of the things I think could help is... Okay, I think a lot of listeners initially think, duh, of course, I handled my security based on risk, and it's actually a good response because it forces the yous and the Is to come [00:20:00] back and go, "Oh, here's what we mean by risk." And I'd love to get your response to that, Mark, is, what does it mean for an enterprise leader of a small to medium, mid-market enterprise to look at their environment based on risk, and be able to convey that to the CFO, the CEO, and whoever their boss may be?

Mark Sangster: Yeah, that's a great point. So, I hit on earlier sophisticated threat actors, we talked about the emergent technology and the technology we adopt, and that's the third piece of that risk equation, is [00:20:30] accountability, right?

Bill Murphy: That's right.

Mark Sangster: And that comes down to managing risks. So, that's understanding what assets you have access to, and who might want to steal them, and what they're worth. And then, also, what your obligations around this look like. So, I think to some degree, there is a bit of an analogy here with the [crosstalk 00:20:48].

Bill Murphy: You talked about this in the book. Why don't you tell the story?

Mark Sangster: Well, it's just that notion of you can't protect everything, so you do have to figure out what it is that you're precisely... What you do [00:21:00] specifically want to protect, and make sure that you understand what the implications are of them going wrong, right? So, building a risk registry. If you can't show me your risk registry as part of that conversation, you're not managing risk. And if you can't [crosstalk 00:21:14]-

Bill Murphy: So, what do you mean by a risk registry? How do you define that for someone? Maybe that's a unique thing for you in your organization, but I'd love to know, how do you define that?

Mark Sangster: So, to me, a risk registry is identifying those critical assets, determining who touches them, has access to them, where [00:21:30] they're stored, and creating at least a top 10 list of what the greatest risks would be. So, is that an insider doing something nefarious? Is that a criminal organization gaining access? And how would they likely do that? And then, having some kind of measure, if it's a one to 10 scale of where your risk stands today, and then a measure of where you want it to be, and whatever the steps are that you're going to take. So, creating a bit of a maturity model. And the reason, it's a simple tool, and yes, we're getting a [00:22:00] bit sort of almost pedantic and sort of the tactical elements of it.

But the simple point of having a spreadsheet somewhere that does that demonstrates that you've thought about it, you've identified those risks, and that you or I, or who else comes into that conversation, can also go to that repository and know that, okay, here's my marching orders, right? Here's the top five things that I got to worry about. I'm going to worry less if this gets stolen. But we can't have these healthcare records get out there, or we can't have our secret sauce to our [00:22:30] manufacturing methodology get out, because if we do, we might lose 30, 40% of our enterprise value.

Bill Murphy: I often think too, I mean, I sold life insurance back [inaudible 00:22:41] college for about four years. And it was great training because I took a beating out there. For sure, I took a beating. But one of the biggest learning points from an analogy perspective is that, someone earning 100,000 a year goes down, and they have young kids or without young kids, [00:23:00] but they're responsible for someone usually, unless they're completely single, but usually there's family dependents in that.

So, that over 10 years is worth, 100,000 times 10, a million, and that's without inflation, that's without any salary increases. And so, that life... And then, not even going out to the true lifespan of that million, but then if the individual... Then you tack in the house and the college expenses, and things like that, that would have to be saved for. But let's just keep it simple at a million.

[00:23:30] If that person then decides, well, I want $100,000 life insurance policy, then they've chosen to accept the fact that the risk that... Everybody's going to be delivering flowers to the church for the funeral, but someone's going to be walking in with $100,000 cheque, 100, one year, but that's a risk decision... Probably, love decision there. But they've chosen not to insure... But then, you losing a life has a certain risk, but then [00:24:00] getting disabled has a higher risk. So, your disability, your chances of being disabled, or bike accident, or whatever it may be, is higher, so you can choose to ensure that risk.

And I'm wondering how often you find people looking at business like, what does it cost you to be an hour out of business, four hours out of business, eight hours? Do people go through that analysis? Do you find people go through that?

Mark Sangster: No, I find they don't, and I think that's a great point. Because you kind of do that cost benefit analysis, where you look at that, and you say, " [00:24:30] Okay." So, with certain types of businesses, or certain types of industry, I should say, things like medicine, you can look up public records of how much the average doctor is... Billable hours are. Lawyers, accountants, any kind of business service like that, right? You know what they are, those industries publish that data.

So, a good example would be a law firm that I did work with after the fact, who was hit by an older version, it was TeslaCrypt of ransomware. They were hit in one site, brought us in, said, "Hey, what would this take? We [00:25:00] explained what to do to protect themselves, and like, "Yeah, no thanks." They moved on, and then they had two more sites hit, they were down for about... I think it was two weeks, 80 attorneys were affected, three court cases were stopped. In the initial period, it was about 500,000 in billable hours. And it was a fraction of the cost to protect that, right?

So, we looked at that, and that's [inaudible 00:25:22] as you say, it's exactly what you're describing in our personal lives, is to say, well, my income is X amount a year, we have this mortgage, we have these debts and liabilities, [00:25:30] if I can't work anymore, and we don't have that source of income, what would it take to protect it, to make sure my family that I leave behind is still protected? They don't lose their home; they don't lose everything else as well. And it's funny when it comes to business, we don't do that. Like what I said, it's suddenly like we think we're in Vegas, and what happens in Vegas stays in Vegas, and we gamble.

Bill Murphy: But you know, what, Mark? The CFO is paying insurance premiums on the building, their paying insurance premiums for unemployment compensation, they're paying all these premiums [00:26:00] to hedge risk, but how often are our IT leaders conveying, here's the cost to mitigate this risk? Here's the things we should not worry about. We should absorb that risk. I think these analogies and metaphors in transferring one domain to another are important, and I don't think we're doing enough of that. Oh, you mentioned reputation risk in the book.

Mark Sangster: Yes.

Bill Murphy: You spent some time on that. Maybe you could talk about the reputation impact?

Mark Sangster: Yeah, absolutely, right? I mean, that's the one thing, is that there's no amount [00:26:30] of insurance that's going to repair reputation. And certainly, if you think about different industries, in particular, I think the trust-based industries is the biggest one. So, again, I mentioned law firms before, this is it, where your clients entrust you... The heart of legal representation is the concept of attorney-client privilege and confidentiality, and suddenly that information gets exposed, that's a hard one to come back from. And at some point, reputation in other ways is... It's not [00:27:00] something you can repair with money.

I tell the story of some airline pilots who were blamed for an event, and they got to the point where flight attendants wouldn't fly with them. And they felt like even though they still had their jobs, it was this horrible, toxic environment. And they got to the point where I think two of the three pilots quit. One became a schoolteacher, another one went to Costa Rica and flew small planes, and farmed down there. Sometimes you just simply can't build back the trust like that. We see the same thing [00:27:30] in investment, with hedge funds and smaller financial institutions where, if you've lost millions of dollars in fraud, that may cause what we call a redemption call, which is... Those very wealthy investors say, "I want my $150 million back because you guys can't manage it properly." And this is the old... Think about the Great Depression, it's the run on the bank, right? Everybody shows up and wants to withdraw their money before it magically disappears.

And it's funny, because you said this [00:28:00] earlier, we do that in a way... In our physical world, we do a terrible job in our virtual. So, we would never park our car in a downtown area where there's a risk of it being broken into without locking the doors and turning the alarm on. But somehow, we use 123456 for our password, for our banking, and we share that password with our email, and our children for our WiFi password. And it's like, this is the equivalent of leaving your Mercedes unlocked in a high risk neighborhood and being surprised when your car is not there [00:28:30] when you come out of wherever you went to, a sports game, or a show, or a restaurant, or something. It's funny how we cannot translate from that physical world into the virtual.

Bill Murphy: It's funny, I have a couple of questions here that I wanted to ask you, one of the... Let me see, before I transition into those though, what are you finding records worth on... You've done through your research on the book, for example, [00:29:00] credit cards versus healthcare records on the dark web, versus social? Again, I'm trying to get into some of the people listening that may be like, "Well, I'm not sure where my risk is? I'm not sure if my staff left how much risk I'm going to be at? I'm curious if you know the answer to that, either through your eSentire background, or the book.

Mark Sangster: Yeah, that's a good question. So, some of these records vary from a couple of dollars, sometimes up to about $50, or to several hundred [00:29:30] dollars. There's a couple of factors here. One is the actual value that it can be resold on the dark web. And the more information they have, it's almost exponential in the value gain or growth. So, if they have your username and your password, that's one thing. But if they have your date of birth, and they have credit card information, or your home address, and so on, all these factors they would use to effectively steal that identity, the value goes up. So, it goes from several dollars up to 150. [00:30:00] And then, from a business perspective, on top of that, you have what it would cost to clean that up, to fix it, it's usually about of a tripling on that. And then, you also have the penalties.

So, if you look at things like the FTC, any of the filings against large healthcare institutions where there's been major data breaches, you're usually paying a fine that's somewhere around one to $2 per stolen record. So, usually, you're talking, say, millions of records here, so you're now talking a couple of million, you usually double that, because you will also have cleanup costs, [00:30:30] and that's the side the companies never look at. When you see these major breaches like Equifax, or Marriott, or something, when the FTC comes along and they find them, everybody looks at the settlement payment, because that's easy. Nobody looks at what's called the corrective action plan, where they now say, "Well, you have to hire a new security person and build out your team, and deploy this kind of technology, and so on."

And as I said, that's usually a 2 to 3X, and it's an ongoing cost. So, when you think of a fine, the fine is the easy part. If you pay $2 million [00:31:00] for that fine for all those patient records, you're probably talking about 6 million in operational liability that you've taken on after the fact. So, it's far cheaper to not have a conviction on your record, I think, than it is to be a felon per se, and effectively have to operate at a much higher cost of doing business.

Bill Murphy: And one of the things that I was reminded of, and actually, I might have learned it, it's a combination of... What was important about reading your [00:31:30] book was, it reminded me of things that I knew, but it gave me a deeper appreciation for the fact, for example, legal world can be a business tool. And then, you can budget for legal expense, because you know you're going to go after someone in the year, they're going to have to go after someone to protect your interest.

Mark Sangster: That's right.

Bill Murphy: However, in this case... Man, I'd love for you to talk about [00:32:00] the nobody's got your back concept and legal recourse?

Mark Sangster: Oh, yeah, absolutely, right? I mean, there's the class action suits that come out of these types of events. There's some recent things that have come out even after the book, but I talk a little bit about, I think, Capital One, where you had 110 million records, credit card records were stolen and exposed. Now, there's a class action suit that's resulted from that, and just recently, the judge in that suit [inaudible 00:32:28] the plaintiffs and is allowing [00:32:30] them to effectively discover and turn over the incident response report. So now, all that information, which is effectively the blueprint for what went wrong, what you weren't doing right, and how it all happened, is now in the hands of your legal adversary. So, there isn't anyone there to protect you. And insurance is only going to go so far.

And I think there's this false sense that somehow if you're regulated, it's almost like you're protected, right? So, well, we have this compliance standard we meet. We're a hospital, we meet HIPAA, or in finance we meet... Pick your alphabet, super regulator, depending [00:33:00] on which aspect of finance you're in, and that somehow because we're meeting their standards for safe. And I have dealt with-

Bill Murphy: Oh, that drives me crazy.

Mark Sangster: Yeah, yeah, and it's [crosstalk 00:33:08] compliance. Yeah, compliance is not security, and it's not privacy.

Bill Murphy: No.

Mark Sangster: Right? There are three sisters, they overlap, but they're not the same thing. I mean, the number of companies I've worked with, where I'm like, "Yeah, you're 100% compliant, you're also 100% owned." Right? And that's the bad news. [crosstalk 00:33:26].

Bill Murphy: The funny thing is... Again, we have analogies for this. [00:33:30] We have auditing standards for auditors, they'll come in and audit your books, but they're following the GAAP accounting principles. So, they know the balance sheet, the income statement, debit, and so it follows a standard. If you're not making money, they're not telling you how to fix it, they're just saying that you don't comply, but they're not telling you how to fix something. And so, it's really interesting how much weight we put in the compliance side of the fence, that's really just [00:34:00] a government regulation, versus actually keeping threat actors out. It's a draw. I thought I was the only one in the world who was aggravated with that, but it sounds like [inaudible 00:34:11].

Mark Sangster: No, no, no, not at all, and it's even the same with... I see the same issue with privacy, right? So, hospitals, for example, they're like, "Yeah, well, HIPAA rules," and regulations, which really designed to protect insider... Sorry, to protect from insiders, right? If you don't have necessary... If it's not a requirement to look and access that healthcare record, [00:34:30] because you're not an attending physician, then thou shalt not look at it, because it's got confidential... Potentially embarrassing, or damaging information in it. That's what it was designed for. It wasn't designed for the notion of some cyber-criminal on the other side of the world who knew how to steal millions of these records, so they can either resell them or defraud some insurer by doctoring up fake claims, right?

So, I think that's the real issue there, is it's almost like, when it comes to regulations, you pointed all your guns [00:35:00] into the center of the fort, and nobody's actually looking at outside. And it turns out maybe, as you said, the wolves at the gate, or the barbarians at the gate, they're willing to come in, and they're coming to attack you. So, there's a different mindset. And the problem also, I think, with some of the regulations is... I tell the story of the Citi corp tower when that was built in the late '70s, and how... Everybody knows Citibank Tower in New York, it's this iconic sort of triangular shaped building. Interestingly, because of some [00:35:30] almost comedic issues around the land that it was built on, it had to be built in an interesting, cantilevered kind of way so that it was literally suspended above a major church that was there on the same grounds.

It passed all sorts of engineering standards. But the problem was, those compliance standards were not up to spec with this new design of this building that was testing architectural and structural engineering limits. So, all the tests that they put it through, it all passed with flying colors. [00:36:00] It was actually an architectural student who was writing a thesis on the building, who discovered that wind from a certain angle would actually knock the building over. And that this type of... The speed of wind that we see comes around every few years in the form of even smaller category hurricanes, and New York gets hit by hurricanes. And they realized this, and it took a little while to expose this, and they had to go back, and they actually secretly retrofit the building. Miraculously, they kept the story... I think the story did stay secret for about [00:36:30] 20 years until it was exposed in New Yorker magazine.

Now, I look at today, I don't think that would ever happen, right? There's just no way... With social media, and the press, and so on, you can't get away with what... The city of New York, and the builder, and the construction engineering firms, and so on, how they all sort of got away with doing this, it would never happen again. But it's an interesting tale for multiple reasons. One of the biggest ones... There are two big things, I think, in this. One of them is what we've touched on here, is that compliance is often lagging, [00:37:00] it's years behind in design. It's not cutting edge, it hasn't thought of IoT, or cloud. And if it has, it's in generalities, but there's no specifics yet that sort of give us the practical guidelines of what to do to protect yourselves, that are proven and tested methodologies.

And then, the other part of it, of course, is the ethical obligations here, which also kind of relates back to your point about no one's got your back, which is, you have to look at cybersecurity as another element under fiduciary care, right? Confidentiality, being transparent, exposing risk to your shareholders. [00:37:30] So, when you discover these problems, you're not... This isn't the 1970s, where you might be able to sit quietly, make it go away, while your retrofit it in the background, this is likely something that's going to come out, that's going to be exposed. And when you do, that could have serious implications for you as an officer of the company, and obviously, for the business. So, you have to treat it as such.

Just as you were saying earlier with CFOs and CIOs, they have great, well understood formulas for understanding risk [00:38:00] and revenue models, we need to apply the same kind of logic and methodology to cybersecurity. And right now, we don't, right? Right now, we throw some money at it, and we blindly trust at the top of the pyramid that the bottom of the pyramid knows what it's doing with that money.

Bill Murphy: Yeah. And the interesting part... We were talking about analogies, and there's a wonderful book called The Checklist Manifesto. And he talks about one of the industries, or the airline industry, building industry, and healthcare, and we lose, [00:38:30] still to this day, 300,000 people a year in the Western world, due to infection caused during surgery. And with the fleet of people in the ORs with these patients, we're still losing 300,000. And the person, Atul Gawande... Atul is his first name, they developed this checklist, and people were horrified that all these smart people that knew all of this about healthcare had to come up with a checklist. And they're still losing [00:39:00] people, but this checklist had made things drastically better.

Then they deployed checklists for buildings, because buildings have all these third-party subcontractors, it's not three people employed by one company, sub upon sub upon sub, they all use checklists, the engineers, all this. And then, in the airplanes, same thing. We were losing planes in the '30s, in the '20s, in the '40s a lot, but now they come up with these checklists. Well, also, everybody... You make a mistake in those industries, you can be sued, there's recourse. We can go [00:39:30] after you for 10, 20, 30 million.

But you brought up a point, which I hadn't really thought about extensively, was, who do you sue when you get breached? I think you mentioned 1% of the people are tracked down and actually sued. [crosstalk 00:39:47] I mean, is that what the fact is? Is it 1% that actually-

Mark Sangster: Oh, yeah, you've got a... Virtually robbing a bank, certainly, [00:40:00] the chance of you actually being caught and prosecuted is less than 1%. Versus, if you walked into a bank with a mask and a gun and held up the bank, there's a likelihood that law enforcement is going to track you down and stop you at the scene, or arrest you afterwards, right? And that is exactly why criminals do this. And this is why cybercrime is bigger than arms dealing, and the drug trade, and so on, because of that. Because if they can operate with impunity, there's a very low chance that they'll be arrested, right? So, [00:40:30] why wouldn't you do it?

Bill Murphy: Yeah, I mean, that's a huge factor, I think. Because in the other industries, you can sue someone. You might not collect the money, but you're going to sue for 10s of millions for malfeasance of some sort.

Mark Sangster: Even that becomes complicated to some degree too, and I think this came out with the Sheraton - Marriott case, because you may have multiple operators in the chain, right? So, it might be a particular brand that you did business with, but it turns out that it's a subcontractor/supplier, [00:41:00] who actually was the one who led to the breach, and then they might be using software that was provided by someone else, and so on, right? We'd call it sort of third-party risk, or supply chain risk, and it's almost an infinite risk.

Bill Murphy: Yeah.

Mark Sangster: Yeah, because it's not a chain, it's like a three-dimensional web. And this is what we're seeing, is suing countersuing. At the end of the day, who gets held accountable? Well, I think it kind of goes back to what we said earlier, well, whose brand is the one in the headlines? That's the company [00:41:30] that is ultimately paying the price of this.

Bill Murphy: Well, you made a big point too, about our governance, outstripping our governance standards. It's no different than Uber, there's no way that the hotel industry or the taxicab industry would have if they knew the disruption that was going to happen from a simple... The Uber app, Vrbo app, because you can download it to your phone, and you essentially [00:42:00] can disrupt an industry by taking over taxis with private drivers. And so, it's interesting, we have very much a disruption right now that there's no governance standard that's going to solve for it. I'm sure the FAA doesn't want drones; they would not have wanted drones. But the impact of this technology is so fast that the government can't move quick enough to account for it.

Mark Sangster: Yeah, it's interesting, right? Social media was kind of the democratization of information for [00:42:30] good or bad. And you're right, you've got the kind of technology that has been almost democratized in some ways, like drones, where you don't need a pilot's license, yet you can cause the same havoc in the skies that you could with a traditional aircraft. And yeah, I don't think they know how to control this yet. I don't think we've thought about it. We often apply the, well I can, so I'm going to, there's never a question of, well, [00:43:00] should we? Right? So, those regs always kind of play a catch-up game.

And you mentioned aviation, and I think that's where cybersecurity could really learn from, because they do have a continuous model improvement like you said earlier with... If you think about what the safety rates look like in the '40s, in the '50s, and so on, where you have bodies that do investigations, that determine [inaudible 00:43:20] were, right? That looks at the confluence of events, makes recommendations, and you have legislative arms that then put those controls in place for all of the players in that ecosystem, right? Airlines, [00:43:30] and pilots, and manufacturers, and so on. We have no equivalent of that in cybersecurity. Yeah, you can kind of argue maybe the FTC, or the HHS with healthcare, but they don't have the same approach. Because it all ends up being resolved in a boardroom behind closed doors most of the time, right?

So, we don't have the access that says, here's all the 50 factors that went into this event, and here's our recommendations based on those. So, you don't have the equivalent of the FAA saying to us, " [00:44:00] Hey, everybody out there who happens to have a digital bank account, you need to do these three things." There's simply isn't that kind of playing field, there aren't the checklists, like you were talking about in healthcare, right?

Bill Murphy: Right.

Mark Sangster: To make sure that medical equipment is sterile, right? There are in some ways, but a lot of it is down to practitioner expertise, and it's almost like village knowledge or something that's passed along through experience and scale, and there's no way of actually spreading that vicariously, [00:44:30] right? Being able to see what happens to one party and be able to infer what you need to do from that moment to protect other parties.

Bill Murphy: Well, Mark, I want to make sure that we give ample time to my listeners to go out and get this book, No Safe Harbor: The Inside Truth About Cybercrime - and How To Protect Your Business. I think that if you're interested in risk... Which I think [00:45:00] all small, mid-market CIOs and CSOs are going to be interested in. I learned a tremendous amount. So, I highly recommend the book. As we wrap up today, what popped in your head that you wished I would ask, or that you wanted to make sure you convey to my listeners that came up from our conversation, that's either related to the book, or just related to the topics we're talking about?

Mark Sangster: Yeah. Like I said, we need to get the [00:45:30] conversation up to the boardroom level, right? It needs to go to the executive level, and we need to talk in dollar signs and cents about risk, not in ones and zeros of technology. But I think the other piece to understand here is that I think a lot of companies are lulled into a false sense of security, right? They don't think they're a target. And when they look at those companies that have been affected, they often blame a single factor, right? They go, "Oh, a server wasn't updated properly, or some security setting wasn't set the right way." As if this one factor is the thing [00:46:00] that went into this event. And the reality is, just like an aviation accident, that there are multiple factors, weather experience, mechanical failures, and so on. And we see the same thing.

So, I think when we just blame an actor, when we say, "Well, a bad guy broke in," we blame the human, right? We miss the chance to look at the systemic issues. So, businesses should be understanding what happened, not who did it, why they made the decisions they made, not just sort of blaming the decision they made, and seeking forward accountability. [00:46:30] So, I think if you don't do that, what happens is... Even the companies that have been affected, as I said, it's a false sense of security. They haven't really fixed the root cause, which means they're probably going to fall victim to it again.

Bill Murphy: Mark, I really want to thank you for coming on the show today, and it's been a great pleasure. How can people reach you proactively, either website, Twitter, LinkedIn?

Mark Sangster: Yeah, absolutely. So, on LinkedIn, it's Mark Sangster, on Twitter, it's mbsangster, and [00:47:00] Instagram is cyber\_ mbsangster. You can also visit me at the website, mbsangster.com. So, that's Mark Bravo, sangster.com. Like I said, I want to change the conversation, right? Get this up to the exact level, and I'd love to continue that conversation. So, I would encourage your listeners to reach out.

Bill Murphy: We'll put links to that on the show notes page. And you work with... How do you pronounce name of the company? eSentire, right?

Mark Sangster: [00:47:30] Yes, eSentire. So-

Bill Murphy: [crosstalk 00:47:31].

Mark Sangster: E-S-E-N-T-I-R-E.com. Is a manage, detection and response firm that works with a lot of different industries, and certainly, has stopped their fair share of nation state and organized crime attacks.

Bill Murphy: Yeah, I'd encourage all my listeners to go check out eSentire as well. Well, I appreciate you very much, thank you, Mark. And maybe we can do a round two in the future.

Mark Sangster: Oh, I'd love to, very insightful, very invigorating conversation. Thanks very much, Bill.

Bill Murphy: Welcome.