**RedZone Podcast Episode #46: Are IT Security Leaders Allowed to Forecast? Become Comfortable with Uncertainty – with Jack Freund**

Jack: For so many years now I can view it in a more general sense of within your life you have to create this list of priorities. What are the top three things in my life that I care about? That's also risk analysis. Those top three things are the most important to me because I'm not willing to accept the risk of not doing those three things.

Successful organizations, regardless of the industry that they work in, view strategy this way: "What are the three things I need to work on? What are the top five things I need to work on? Is everything I'm doing driving me towards one of those things?" In security, where we have so much to fix and so many things that can go wrong, we need to be willing to sacrifice the small things to work on the big things.

[00:01:00] I had a boss at Nationwide years ago. One of his favorite phrases was, "I don't want to major in the minors." I love that phrase because it's exactly the right thing. What are the big strategic things that I need to knock out. I think that FAIR gives organizations large and small a tool set to be able to think about and talk about security issues and risk and strategy in that way.

Bill:

[00:02:00] We have Jack Freund on today. He and Jack collaborated on the book called FAIR, A FAIR Approach: Measuring and Managing Information Risk. Although I know you and I, Jack, aren't going to spend a ton of time on the book, maybe just for our listeners you can give an overview. I'll link up the book on the Show Notes page, so that certainly will ...

This is a bible for IT security professionals, CIO, CISOs. This is a great tool for one's self as a leader, even just to get an overview, and then for the security professionals and risk professionals, definitely a huge benefit for their library. The book, in essence what does it do for people that you've had your biggest reaction from your readers about?

Jack:

[00:03:00] The book is really the product of the work that Jack Jones had did when he created the FAIR Methodology. Through my work with him, I've learned a lot about that and had the opportunity to expand it and create some unique applications of it. I think the book really gives people a foundation of language in which to talk about and describe risk.

It is also a calculation method for how to compute risk. I think it's a problem-solving book, "How do I take all these things that it have to worry about, all these things that I have to care about, and how do I boil them down to the things that matter the most to me?" The one thing, to answer your question about what the biggest reaction is, people sort of find it refreshing to think about risk in this way.

One of my mentors, I would say, one of the people who I admire the most is Douglas Hubbard. We, Jack and I both, have borrowed a lot from his work in how to measure risk this way. He has a quote where he says, "What we don't want to do is create ..." and I'm paraphrasing, "We don't want to create our own special, secret way of thinking and talking about risk that only applies within IT.

[00:04:00] What we really want to do is be able to talk about it and apply it in a way that other risk professionals in other disciplines can understand too. In my time working for larger organizations that have a mature enterprise and operational risk function, I found this to be true.

When you start thinking and talking about risk in terms of expected loss with ranges and other statistical methods of error bars and that kind of thing, you really begin to see people understand it in a way that wasn't necessarily there. It gives people the ability to bridge the gap between being a highly-skilled, very-technical security person to gain access to the way that business professionals think about technology and risk associated with it.

Bill:

[00:05:00] Yeah. I found that myself just reading it. I often have to speak in front of boards. I'm often brought in my the CIO or the CISO to really kind of a show-of-force, especially if those CIOs haven't had as much interaction with the board from the IT security side.

It's very, very useful, the book, from the concepts and the metaphors and the way in which it really almost enhances the maturity level of the discussion by the concept of risk, and helping to kind of demystify.

I think also to get people out of fear. I think the refreshing piece is that it's almost like stepping outside of the fear-brain for a moment and really looking at it more logically and defensibly, the message that's trying to be conveyed by the security organization.

Jack:

[00:06:00] Yeah, I think you're right. I like that [inaudible 00:05:56] that you said about stepping outside of the fear-brain. I think in general the way we think about risk, regardless of topical area, is "How do we not have any?" I think many people probably go through life with the unconscious assumption that they have the ability to never die. We don't, as we all know.

It's really about, in a very morbid kind of way, "What are the things you want to minimize in your life to avoid dying in certain ways?" I think, when you start thinking about life as inevitable failure to a certain degree, when you start thinking about business as "Not everything we do is going to be successful," when you think about security as "Not every control we put in place is going to work 100%," then you start thinking about things in the middle.

[00:07:00] One of the phrases I use is "Becoming comfortable with uncertainty," that's a very different way of looking at things. When you talk about presenting to the board and that kind of thing, I find it wholly unreasonable to expect security professionals to educate the board to become security professionals. They can't. They're experts at managing businesses. They spent 20, 30, 40 years becoming that.

We spent that same amount of time being good at what we do. I think it's incumbent upon us, if we're smart enough. We claim that we often are. I see this all the time, this sort of "Those dumb X, Y, and Z; they decided not to do this, and therefore that's a bad security decision. I don't know how they could do that."

If we're that smart, then why can't we bridge the gap and learn to think about the business and risk and security the way that they do in terms of, "I know that something bad will happen. I can set money aside in a reserve fund in case it does, but is the cost of that bad thing happening so great, so high that it's unreasonable?"

[00:08:00] If we can answer that question, then we can begin to have a reasonable conversation with them. That's what I hope the book helps people to do is, while paying homage, of course, to the deep technical knowledge that's necessary to be a security risk professional, also to understand and extend your view into "What's the ultimate goal here?"

Offering a product or service for money, if you're a non-profit organization, if you're offering that product and service, it in general is itself a risky venture. The business is inherently enveloped in risk all day long. This is just another vector from which bad things can happen. Aligning the way that you think about risk and the way that your greater organizational forces think about risk is essential to having meaningful conversations with them.

Bill:

[00:09:00] Yeah. I think what's really interesting it's almost ... The book is deeply technical, but I found these amazing metaphors for risk. It's funny. You no longer can embed these conversations in just the risk department or with the auditor; it's bubbling up into the board. The context of the language-ing has to shift because the board is not really able to hear the message.

I love your statement of becoming comfortable with uncertainty. It's uncertainty from, really, a couple of levels. It reminds me of an author [inaudible 00:09:29] who writes about being comfortable with discomfort of the risk, but being able to have a language where you can have really adult-orientated conversations without really moving into, again, this kind of irrational thinking about purchasing, potentially, more shiny toys to solve risk instead of really looking at it from a more logical point of view.

[00:10:00] Your blog posts ... Recently I've been doing a lot of reading on your blog and your work through ISACA and ISSA. I'm going to put links to your blog and the ISACA article and also the most recent one you did, which you have a great slide show presentation. You really talk about "Risk work is never complete.

The continuous improvement should be the goal. Almost embracing being incomplete." How does someone take that statement of continuous improvement and convey that to business so they know that risk is not something that is static, but it's actually moving and can be a moving target? How do you actually convey that to the business?

Jack: I think it's a very mature place to get to to be able to have that conversation. It takes effort. I think in any organization that's looking to improve quality in the work that they do, they kind of have to approach it the same way. When I started writing about risk-assessment quality. I was sort of thinking about, "How do I know if I'm doing this right?"

[00:11:00] Some of the mathematical work that deals with this kind of thing ... I'm not an expert in math, but I have people that are. This is what they tell me, is "You have to measure what the real results are against what the expected results are." The best way I've found [to 00:11:18] find that was to use data that was available to you.

I think a lot of organizations don't often have great data inside of them, but if they do, if they have infinite data, then that's a good source for that. If you don't, there's a lot of great industry reports out there that you can use to help measure that. That's what I was trying to do, is how to take the results of this.

[00:12:00] When I say that this system, this application, this service database is high risk, how right am I at that? If something were to happen a year from now, would I still be right that it was high risk? I think that is one of those internal measures that you begin to build that allows you to say, "I'm doing this in a correct fashion." [inaudible 00:12:04] started, again, from Douglas Hubbard's book: How To Measure Anything, when he talked about what he called forecast accuracy.

Bill: Sure.

Jack: There's some really great equations that can help you with those kind of things. We don't have enough data, enough ability in the things that we're doing right now with risk data to be able to get that precise with it. Meteorological forecasting, for example, uses Brier scoring. If you say that it's going to rain, that it actually rained; very binary, yes or no kind of things. That was sort of the approach that I took with this.

[00:13:00] I said, "Can we build these formulas that say, 'When I said that we expect cyber criminals to attack us once every two years to once every three years, how right was I?'" We can sort of take that view, that window of our event-forecasting and look backwards and say, "Okay. Over the same time period, how many internal incidences did we have that related to that particular attack vector?"

Then compare them again to external data, "How often did this report say that, for people that look like me within the financial services industry, for instance, how often were they attacking us?" and produce variance charts that say, "Hey, I think we're underestimating our risks this way. I think we're overestimating our risks this way." I think it's really kind of fascinating.

[00:14:00] It provides that justification for how you take it the business and say, "Look, from the best data we had available at the time, we were pretty confident that this was high-risk. Now we've seen this up-tick in attacks, this up-tick in losses. As a result of that, we need to revise your entire risk portfolio." Whereas before you may have only had one application that was high risk, now it turns out that the attack frequency has gone up and class-action lawsuits have risen as well.

As a result of that, these things are now all going to be high-risk. That's, again, a very mature conversation that's deeply indexed to what's going on in the world around us. I think one of the go-to conversations that you end up having with executives around security is, "What's everybody else doing?"

Bill: Yeah, that happens a lot.

Jack: It does. While it sometimes frustrates me, this sometimes gives you that view into, "Well, here's what we think is actually happening elsewhere." I say it's frustrating because it's difficult. You don't really want to have a chatty security organization that talks about all of its happenings and all of its control-failures and that kind of things.

[00:15:00] There are mature industry forums that allow you to have those conversations off the books, but you're never going to know the precise configuration of controls at your competitor or you're never going to know the exact frequency of attack that they're seeing, if they're measuring it at all. You have to have something to kind of work with.

This, I think, is a really good proxy for that. It gives you the base measure of how good we think we are at estimating what losses are going to look like and how good we are at estimating what frequency-of-attack looks like. Underlying all of that is the need to have standardized ways of measuring and managing risk. I think that's really where a foundation like FAIR helps with that.

[00:16:00] When you're calling certain types of attack cyber criminals and certain types of attacks [nation-based 00:15:45] it has to be uniformed and consistent. When you're measuring frequency, it has to have meaningful application within your organization. This is really the things that our staff and I wrote about in the ISSA article and that the slide-show presentation talks about. Those are really add-ons for, once you have started building FAIR into your organization and doing risk-assessments, here's how you take it to the next level.

Here's how you being answering that biggest question that we often get when we start to implement FAIR, which is "Where am I going to get this data from?" This is one of the ways that you can do that. You can tune the rating tables that you're using. You can gather data internally and externally and compare that, index it, and really have your finger on the heartbeat of what's going on within the organization and in your competitors as well.

Bill:

[00:17:00] If you were a CIO ... A lot of our listeners are going to be CIOs that are going to be also wearing that hat as the CISO as well. As well, there's going to be not that audience. There's going to be pure CISOs that are listening. I'm always struck by the conversation: what others are doing.

If you walk in with a top-ten list, which seems to me to be not a very useful list to walk into a decision-making [inaudible 00:17:09] "I would like to purchase these products, these services, these staffing changes. These are the top ten areas." If someone wanted to, from a very simple point of view, how would they go about ...

How would you walk them through evaluating the probability and the potential frequency of events happening that you were hoping this top-ten list is going to be needed for? You could you reverse and quickly coach someone through a process more down the model that you're explaining with your approach?

Jack:

[00:18:00] I think that desire ... I'll just address this broadly. I think that desire to say, "What's everybody else doing?" is a proxy for "I think this other organization is managing themselves really well and I want to be like them." I think that is usually born out of the fact that people tend to discount their own data in their own organization.

There's that universal truth that we've all experienced where you're much more knowledgeable about security when you work outside of an organization. As soon as they hire you, they need to get outside people to help consult with you about that. I always find that funny. I experienced a similar thing when I was consulting for State government years ago.

The State really thought that private industry had security down cold. [When you get 00:18:28] to pollinate between both of those kind of organizations, you're like, "Yeah, maybe not so much." If you get to this point where you find that there's a particular technology aligned to your standards and policies that you think would really help drive change in the organization and improve the risk profile, you have to talk about what the reduction of risk is going to be.

[00:19:00] Often times we're in this [quick-zotic 00:19:00] search for ROI in the security industry. I've never been a fan of that term because, again, if you think about the way that true investors think about ROI, your investment in [Evincia 00:19:15] as an example, they're not going to pay you out because you avoid certain types of security incidents.

There's no cash payout at the end of that. At the best you can do cost-avoidance, which I think is almost the same thing, but philosophically different enough to really allow you to think through the problem the right way. If you can say that "We think we're experiencing incidents at this frequency," ... FAIR helps you break that down.

[00:20:00] If you don't know loss-frequency, you can begin deriving it from saying, "Here's how often, I think, that we're attacked," and "Here's what our control [inaudible 00:19:52] looks like, how vulnerable we are to these types of attacks." If out of ten attacks, you think that nine of those ten are going to get through, then you're 90% vulnerable to that and you reduce your threat of frequency from that.

When that happens, you can say, "Well, okay. If we put this technology in place, I think those nine attacks that are getting through out of ten, that might reduce to two or three." Then you can see how that cascades down through the rest of the equation. If we're experiencing less attacks, that's less time and money we're going to spend responding to it, that's a lower frequency of lawsuits, a lower frequency of fines and judgments, a lower frequency of payouts to customers depending on what kind of a business model you have.

There's less bad things happenings on the other side of that, less cash that really will be out the door. These are all future dollars. We haven't actually spent any of this money yet that we may or may not experience loss for. What you're saying is "I think that if we do this, we're going to have ten less incidents over a ten-year period.

[00:21:00] As a result of that, there's a certain dollar amount that we can forecast as being associated with that. That's my stock go-to for justifying investments that way. Actually that same kind of approach can cascade up, too, to larger strategic initiatives as well. It's not just "I need to buy a box of X;" it's "I need to invest in a full, end-to-end, user access, [entitlement 00:21:21] review system. I need staff to do that. I need processes put in place."

You can begin to sort of justify your strategy for all of your cybersecurity activities in the same kind of way. Incidentally, this isn't just specific to cybersecurity; you can do this for a lot of things. I need to invest in a new web platform because I think customers are going to use it more, as a result we'll experience an increased amount of transactions which has revenue associated with X.

Bill: I think this is really good. I think this is really interesting. Sorry to interrupt you, Jack.

Jack: No, that's fine.

[00:22:00]

Bill:

I'm getting excited about it because you never see the VP of sales come in and say, "I will deliver $40,000,000 in sales to you this year" to the CEO. He's saying, "I'm forecasting $40,000,000 sales," then list out the channels, the analysis done to support that figure.

I'm always struck, particularly, by one of your slides in your presentation which was the difference between prediction and forecasting. Maybe you can just explain that really quickly. That's sort of what you just walked me through, which I found interesting, but maybe you can make that hyper-aware for everybody, what you meant there.

Jack:

[00:23:00] Yeah. This is one of my favorite topics. There was a point when I was doing FAIR training with Jack where he made very plain, "We shouldn't call this prediction." I sort of had this cognizant diffidence about it because, if I wanted to do that forecast accuracy, if I wanted to go back and look at how good I did at putting these rates around frequencies, I thought, "Well, if I'm comparing what I thought actually happened to what I said was going to happen, aren't I really predicting something?"

Then I came to the conclusion that I don't think it's about logic. I think it's just about impression. I think prediction has a very negative connotation. It really emotes thoughts of fortune-telling and that kind of thing: "I am predicting that we're going to have incidents that look like this."

I think forecast, in business language, gives you a little bit more wiggle room. I think people allow you to be wrong when you have forecasts within certain tolerances. I think that's really what we're talking about. On the slide there I included a picture of Hurricane Rita. I was thinking even some of the best mathematical forecasts in general can't predict where exactly a hurricane is going to land in a couple-hour time-frame.

[00:24:00] That's just because of the very difficult nature of how those things work together: all the different systems and the weather patterns and how they interact and land formations and air temperature and moisture. [inaudible 00:24:14] while fundamentally different, it still has the same kind of complexities to it: how often people attack, whether we're in the news or not, the state of our controls at that particular time.

There's so many things for which there's variability. We can't predict anything, but I can forecast it. Again, I don't think it's a logical difference necessarily. I think it's really more about being open to ... Like I started with saying, it's being open to being comfortable with uncertainty. I think forecast allows people to wrap their head around being comfortable with that versus prediction is almost like a challenge.

[00:25:00]

Bill:

Yeah, it's so much more positive. I think it's a much more comfortable business-speak for people. You can be a serious risk professional and IT security professional and change your language to a point where you're ... This is where I love the practicality of being able to communicate with decision-makers with this language.

I think what you're emoting is deep logic and reasoning and analysis, but you're taking the conversation to a point where human beings can understand it who may have a wide and varied business background.

You're bringing it into a language that even they understand, that even sales understands. I think that's so important in the security arena because we have to make the underlying assumption that deep thought is going into the analytics, but when we're coming out, how are we presenting this information? I think what you're saying is really important.

[00:26:00]

Jack:

Exactly. I think there's a big difference between the type of skill-sets required to successfully compute risk and the type of skill-sets required to communicate risk. This is one of those key things, is knowing the difference between when to use certain words and when not to use certain words. The thing about forecasting is it's already a term that's widely used in business.

We make budget forecasts. We make expense forecasts and Excel forecasts. People know what that means. There's not a high expectation of accuracy associated with that. I think that's one of the things that this allows us to do. Regardless of whether we forecast or predict risk, a decision is going to be made one way or the other.

[00:27:00] If you're not at the table to have that conversation, to take all that good analytical, technical work that you've done and say, "Hey, based on what I know and based upon SME-expertise, I think we need to do this," if you're not even at that table and you can't have that conversation in a way that business understands, nothing is going to get done.

Even if you have to bring to them something that lacks the precision that you may hope for, a decision can still be made and we can still move forward and we can still appropriately protect the business or, at the very least, make the business aware of the choices that they're making so that they can make an intelligent decision.

Bill: A couple clarifying points that I was hoping to talk to you a little bit about is that I find it fascinating. I'd like our listeners to be able to literally walk out of their car and be able to take action on something they're listening to. One of the pieces I think that's really interesting that I think could really help immediately is how you integrate external data into your analysis.

[00:28:00] You're coming up with a reason how to justify the spending within the organization, IT security spending, and you've done a risk analysis, but the piece that I'd like you to spend some time on is how you integrate external sources of data so that it doesn't become too complex, but makes a cogent point either regarding competitors or regarding the industry that you may be in.

For example, if you are a pharmaceutical company, what would be the steps that you would walk someone through to evaluate these external sources to support a decision they want to make?

Jack: Yeah. I think you have to find good sources of data to pull from. I think there's a lot of really good ones out there. I mentioned the Verizon Reports. One of our favorites is the Privacy Rights Clearinghouse. [inaudible 00:28:53] a pretty good one too. They have a for-profit model now, but they're also a really good source of data.

[00:29:00] It's really just a listing of bad things that happen at other companies, and it has data associated with it, so you can inherently get frequency from that. You have to spend a lot of time massaging that data. That's what take a little bit of effort, is taking those reports and looking at how they classify business types.

Pharmaceutical might work well for you, but if you are in the durable goods business and not necessarily in the pill business, you have a different model and you might decide that that's what you think you look like or what you don't think you look like. I've found that most companies sort of have this running list of who they think their competitors are.

[00:30:00] Sometimes it's an aspirational list. If you're a mom-and-pop grocery store, sure, Walmart is a competitor, but not exactly in the same level as you. You may be losing business to them, but maybe not so much. From a breach perspective, you have to think about in terms of "Who are the attackers targeting?" If [want to target 00:30:00] the top-five banks, that's a different kind of target than everybody who happens to be in the financial industry.

You're going to get credit unions and much, much smaller organizations that might not have the same panache. You have to think about that and, as you go through the data-sets, find those organizations that are like you that business can relate to. "That looks like me; therefore I understand the risks better," is kind of the thinking with this.

Bill: Okay.

Jack: When you do that, you have this innate list of, "Here's the frequency." You have Roche Diagnostics. I'm trying to think of a pharmaceutical company off the top of my head. You have this list of companies that may have incidents associated with them regarding data-loss and theft, for instance.

[00:31:00] If you time-box this into a year, you can say, "Okay. Across all of our competitors I found five examples of things that have happened, so any one of those five competitors is only having one event per year," but we have a larger list of competitors that we care about; there's ten, so maybe that number looks closer to point-five, one half a year for them collectively. You have to compare that to the rates that you're using.

If you're not using those rates, if you don't have those rates established currently, then you can use those to inform that better like, "Well, if we look anything like them, this is what we can expect our losses to be in the same way." The same thing works on dollar-losses as well, though you tend to find much less data associated with that. When you do, it tends to only be a certain kind.

[00:32:00] In FAIR we talk about six different types of loss. The ones that tend to get published the most are fines and judgments. The other ones you have to spend some time inside your organization coming up with rates for that kind of thing. Sometimes you get legal fees and response costs as well. In any case, once you have all those things established, you can begin to build these sets of rating tables, as I like to call them.

Just like you would rate teenagers that are driving cars differently than you would pensioners in Florida, you have different profiles of what frequency-of-attack looks like within your organization. That data becomes very strongly linked and very strongly indicative of what you think that loss and that frequency-of-loss and management-of-loss looks like for your organization.

Bill: Do you ever wait ... For example, intellectual-property-loss, is that something that is harder to calculate? What are your thoughts on IP-loss that may not be necessarily something PCI is going to pick up on from a PCI audit? How would you approach that?

[00:33:00]

Jack:

There are things that ... I tend to avoid hard or difficult to measure as a phrase. I think there's measurements that have much more variability in them. Things like reputation-loss have that kind of thing. In some of the courses I teach, I'll sometimes post this theoretical conversation around, "What's somebody's life worth?"

Usually when people, their jaws close and their eyes stop bugging out of their head that I would ask such an impertinent question, we tend to have a pretty rational discussion around it. I was consulting for one financial company years ago, and we were teaching them FAIR. I asked the same question. Everyone was mortified that I asked that question.

I was like, "Well, don't you sell life insurance? Aren't people actually putting a price on their own life?" There's different ways that we do that. Certainly that price is never going to account for the emotional attachment you have with loved ones and things like that, but there is a way to do it and there's variability in that certainly.

[00:34:00] Court proceedings do the same thing all the time. You have these damages that happen. Organizations like the EPA have rates associated with loss-of-life. When I think that we can solve that problem: I can put a price on Bill's head as an example, I think we can solve other problems too.

We can measure things like, "If this key patent that we rely upon, if the underlying research associated with that were to be disclosed, how would that effect our organization?" I think to answer that question you've got to get the right people in the room. Most of the time the right people are not security professionals; you've got to talk to the people who are trying to market that and trying to get it out there and trying to monetize it.

[00:35:00] If you could do that, then you can start answering simple questions like, "Okay. If we couldn't rely on this IP anymore, if our research was disclosed before we were able to file, for instance, how would that effect our business?" It typically boils down to a couple not simple, but straightforward questions.

That's "How many less customers are we going to have? How many customers that we currently have are we not going to be able to retain? When and if they chose not to do business with us, how much money do you think we're going to lose?" I would expect wide ranges with this. You should estimate it using a mid-max-mostly-likely kind of thing, so "What's the most we can lose? What's the least we can lose? What's the most likely?"

When you can start having that conversation, you sort of back off the cliff a little bit and begin to rationalize, "Okay, here's why this is important." I think that's one of the key things. I offer the whole discussion around putting a cost on loss-of-life because that's a hard problem.

[00:36:00] How do you reconcile the emotional impact of the loss of a loved one? If we can do that around that, I'm sure we can do it around business-process patents, I'm sure we can do it around copyrights. I guarantee Disney has a pretty good view of what that's going to cost them if they ever lose the copyright on Mickey Mouse, as an example.

Bill: On your latest journal that you published [on 00:36:11] protecting data against cyber attacks in big-data environments, I was just reading that through. You talked about data coding and cleanup. I know I'm kind of picking on one area. I was just curious what your perspective is on this. Where does this fall from a risk point of view in your mind as far as does this get into more assessing an asset itself or just general coding and data coding and cleanup within the organization?

Jack:

[00:37:00] I think I'm talking about it in particular regarding using external sources of data. These are often times volunteer efforts and sometimes the data is just wrong or not applicable. I think broadly speaking, when you're building these sort of analysis tools and you're relying upon ... I don't know. Let's say you're company is CMBD System, this repository of all the IT resources that we care about.

I think there's a different view of "I can only assess what's been given to me," that old line about going to war with the army you have. If the data is wrong, and it's probably wrong to a certain degree or another, I think you can really only be held accountable for the things you have in front of you. If the response back from the organization, for instance, is "You said this server is high-risk because it's externally-facing. It's not."

[00:38:00] "Okay. Well, I got that data from the CMBD. We'll go ahead and fix that and we can update that risk profile to reflect that." At a more meta level, you would have to estimate "How many systems do we think have data elements associated with them that I think would cause them to under-rate the risk and then over-rate the risk?" and "To what degree is that going to effect losses that we might experience with that?"

If we under-rate the risk, are we not going to prescribe controls for that system that has a certain amount of loss associated with them, so we'll be exposed to additional loss because of our data-coding problems. I think there's ways to do that. That particular scenario is probably a little more high-level, but it allows us to sort of categorize what we think risk looks like for a poorly-maintained CMBD, for instance. Does that answer you question?

Bill:

[00:39:00] Yeah. Definitely. I think it's just important, I think, for the people to know that, when they're pulling the data-sets in ... I'm going to link up to your ... I find your presentation really useful to understand the method of how to do this. ... being able to pull in from the sources of data, that it's not always clean, but that they go through this process and make it better.

Jack: Yeah. That's one of those things that, any time you start working with large data-sets, especially data-sets that you don't have direct control over, there's always going to be some coding problems with them. One thing I learned from Social Science Studies, they have a technique for coding things.

If you have to categorize something, you could just have one person do it, but in order to increase the accuracy of it, you have multiple people do it. If you have more than one person on your team go through the same list and say, "I think this looks like a insider attack. This looks like an external attack," especially in those external data-sets you get a lot of ... Sometimes they're very terse.

[00:40:00] Sometimes the descriptions are very long and they contradict what the categorization says. If you have a couple of people go through that data: "It sounds like an insider attack. It sounds like an error to me. That sounds like ..." these kinds of things and you compare that across multiple people, you increase the quality of that data before you begin to do any sort of work with it.

Bill: I really like the ... It was an interesting chart to choose. I'm a real big proponent of visual charts. You make the differentiation between privilege insider breaches and non-privilege insider breaches. I find it really interesting how you pulled the information from external sources to be able to say, "Okay. The privileged insiders accounted for X% of breaches."

Then you compare it to non-competitors. Who would be asking that type of a question, do you find? Does that come back to our original statement which was "What are our competitors doing?" or "What are other people doing about this?" or "Who's currently experiencing thing problem as well?"

[00:41:00]

Jack:

Yeah. I think there's a couple of layers to this. The first is the distinction between privilege and non-privilege really comes down to one of the factors within FAIR that we use to analyze the risk, that's where you apply your preventative controls. Within any organization, you're going to have a certain group of people: UNIX admins or BBAs, that really have the keys to the kingdom.

They can do anything the want. The only thing that's stopping them from doing that is that they don't chose to do it. Every time they attempt to do something bad, they're going to succeed because we've already invested in them the rights and privileges to make that happen. That's the big distinction we make between privileged and non-privileged insiders.

[00:42:00] The privileged are the people that you really worry about not because they do anything with any sort of frequency, I hope. If you have a very high rate of privileged insider malicious activity, you probably need to look at your hiring practices. In most organizations I've consulted with on this, there tends to be a very low frequency of attack.

Just ballpark, most companies put that in one-in-ten, one-in-fifteen, one-in-twenty years event. When that happens, it matters a lot because you can lose a whole lot from that. The rest of your organization that doesn't have direct access to anything really damaging, we lump into that other category of non-privileged insider. They have to overcome some kind of control to be able to make their attempt successful.

At FAIR we call that the difference between a threat event and a loss event. Loss events are basically incidents at that point. What do they have to overcome? Do they have to bribe somebody? Do they have to be granted access erroneously? Do they have to hack into something, get somebody's password? All those kind of things serve as friction to keep them from doing back things.

[00:43:00] Those charts you mentioned are variance charts that I think are great visualizations to accompany that message to business that says, "Hey, we're constantly keeping our finger on the pulse of the security industry. Based upon this latest report, here's what we're seeing. We're seeing this rise or fall in events of this type."

As a result of that, you can go on to have that conversation around "The ten medium-applications in your portfolio are now all high-risk," as an example, and "Here's sort of the reasons how we came to that." I think too much we consider risk-assessment a one-and-done kind of thing where that overall risk rating is what it is every year year over year. It doesn't have to be.

[00:44:00] I think that's a measure of quality, is how you're adjusting that in tandem with the changes you see in the organization. We spend too much time focused on controls in particular. This is really sort of a different look at this, is "How often are people doing things that we need to care about?" That distinction between competitor and non-competitor is exactly to answer that question of "What's everybody else experiencing?"

It's one of those things, I think, that business looks for in your presentations and in your manner of speaking to see if you get it. If you're really thinking about competitive advantage and competitive concerns, I think they really believe that you understand the business that you're in with them and they take your recommendations more seriously.

Bill: Yeah, I guess it does convey a bit of depth of review, but I think it's a different depth. When you look at competitors and you look at external sources, like you said, you're not just trying to deepen the analysis of controls, but you're actually looking at the landscape to look at the likelihood and the frequency of these events happening.

[00:45:00] It's like if I had five buildings to insure and I had different premiums for an insurance policy to look at, I could insure for different levels of risk, I would want to know what the differences are from the premium payments I'm making. One might be just insuring for crater-in-the-ground events. One might be insuring for water damage. One might have different variabilities. It makes sense. It totally makes sense for a business decision-maker to look, "Okay. I'm spending this amount of money, but what is the risk I'm mitigating with this?"

Jack: Absolutely. As the insurer, you would want to know if there was anything you could do to lower your premiums. Right?

Bill: Correct.

Jack: "If I behave this sort of way, if I included this additional control, would you lower my rates?" Again, that's a metaphor that business understand. If you start characterizing and casting security concerns in the same fashion, they get it, they can have conversations with you about it.

Bill:

[00:46:00] When we started off the conversation ... This is prior to when we started recording. ... we were talking about the most important things to work on. We didn't have an unlimited budget, there's not an unlimited amount of time, and people can generally get very hyper very fast about security and security spending. You had an interesting philosophy and a question that you asked that was about focusing on the top three things. What was the question you feel that a security professional needs to ask in a time when we don't have limitless resources?

Jack: Security professionals need to ask, "What are the most important things I need to work on?" because you're never going to work for an organization that has an unlimited budget to do all the things that they care about. They don't have an unlimited budget to do all of the marketing activity that they want, all the product launches that they want, all the new acquisitions that they want to do.

[00:47:00] You have to sort of take the same approach to managing security. You have to look at "What are the things that we can do to make the biggest impact? If I only had X-number of dollars to spend, would I spend it on mitigating insider attacks or external attacks? What does the data tell me?" You have to be dispassionate about that and be willing to overlook security folklore, "Insiders are our greatest risk" kind of thinking.

Look at "What does the data tell you? Do you work in a business where that is actually true or is it something else?" [Half of 00:47:32] those priority, I think, are really important. Any time you have to create a punch-list of the top three things that we care about, whether it's security concerns or whether it's a list of priorities and what you want to accomplish, priority equals risk every single time.

[00:48:00] Those are the top three things we care about because we're not willing to accept the risk of not doing those three things. You have to think about it the same way: "How often am I going to experience loss associate with that? When I do, how bad is it going to be?" You have to make sure that all the strategic things you're doing and all the tactical things you're doing align to those top-three things.

We are managing our top risks because we have these programs in place and we have these daily processes that run to make sure that we're managing risk in this fashion. Aligning all that allows you to say very confidently to management in your organization that "We get it," and "We see how these top-three things effect our overall risk profile," and "We've indexed them to impact on business-objectives," that's a very powerful way to run your security organization.

Bill: I really appreciate you for making that distinction, Jack. This is a great way to kind of bring this to closure because it seems obvious, but it's not.

[00:49:00] I think sometimes we can get so harried with the amount and volumes in our life that we're tackling professionally that it's very difficult to sometimes distill to the core three, of which then you can use your model with the FAIR model and your approach of using outside sources to support data for frequency and how bad the loss will be.

We can lose that in the lot. In the volume, we can lose the fact that we need to be simple and focused on the top three. That is a great summary, so I appreciate you for that.

Jack: Yeah, thank you.

Bill: Jack, thanks very much for coming on the show. I really enjoyed talking with you. I know our listeners are going to get a lot our of this. I'm going to link up both your presentations, your blog, LinkedIn profile, and your previous work for your writing. Is there anything, as we wrap up, that you want to share with our audience before signing off?

[00:50:00]

Jack:

Yeah. I'd just point out that this past April 5th Jack and I were inducted into the Cybersecurity Canon. The book that we wrote was selected by Rick Howard, the CSO at Palo Alto Networks as one of the books that cybersecurity professionals must read. It was a great honor. They put on a great show there for everybody.

They treated us very well. It was nice to interact with some of the other authors that won as well. I think it's also external validation that what we're talking about and what we're writing about matters a lot and that people get it and they understand that this is really solving a problem that we have as an industry, so ...

Bill: It really is.

Jack: I thought I'd point that out.

Bill: Yeah, it really is. I really deeply appreciate the work you're doing, Jack. I know Rick Howard quite well. He's been on the podcast last year. He's a power-packed individual. He's a lot of fun to talk with.

Jack: He's a great guy.

[00:51:00]

Bill:

That's a big win for you guys and the book. I highly encourage everyone to go out and get a copy of it. Thank you very much, Jack. Hopefully we can get you on for round two here sometimes in the next twelve to twenty-four months.

Jack: I'd be happy to come back. Thank you, Bill.

Bill: Thank you, sir. Take care. Bye, bye.

Jack: Thanks.