[Introduction]
With the rapid behavior changing disruption of recent years, and the ongoing stream of corporate governance failures. ACCA has been digging deep into how interconnected risks such as climate change and geopolitical issues are influencing the way we approach risk management. This podcast series will look at what risk culture means and to what extent risk and accountancy professionals understand its impact on performance.

[Rachael Johnson]
Today, we are delighted to welcome Nick Sanna back to the ACCA to talk about cyber security, and this time, given our current research on risk management in healthcare, we are going to delve into how our members in this sector can do more to help their organizations deal with these growing threats. So as the founder of the FAIR Institute in Washington, DC, and President of Safe Security, let's start with the story behind fair and what Safe is all about, too.

[Nick Sanna]
Thank you for having me, Rachel, in terms of the story of the FAIR Standard, which is a model to quantify and account for cyber risk, from the financial perspective, from the accounting perspective, it came about when a chief information security officer in a insurance company was meeting the board was basically inquiring and overseeing cyber risk and asking basic questions such as, how much risk do we have, and if we give you those $20 million to secure our environment, how much less? And he felt like that he was not equipped to answer those questions in tone. He was ready to talk about threats and vulnerabilities, which were more technical in nature. But really, what these executives really needed to understand is, what is the impact on organization, and how much of an investment will be sufficient to get to keep us out of trouble. And he didn't have a means to do that. And so that was the the spark that led to development of FAIR which is a way, again, to assess cyber risk from the financial perspective and also to measure controls effectiveness in terms of risk reduction.

[Rachael Johnson]
So this time last year, you presented to ACCA CROs and heads of risk forum about what's driving the evolution of quantifying risk management, or quantification risk management in cyber and operational risk. But boy, a lot has happened since. So could you tell us about your new model for assessing and accounting for cyber losses, and again, in particular, how this would apply to healthcare?

[Nick Sanna]
Yeah, absolutely. I think this is a very important topic. So the FAIR Standard has evolved, and we now issued, in the last year, the FAIR Institute a new standard called the FAIR materiality assessment model. And so what this model really does, it provides a way to decompose cyber losses in categories that would make total sense for a CFO or a cyber insurance company. And so they'll give you at a high level, you know. And again, this model is called FAIR. If you look at the FAIR Institute, you'll find references to it, but it really breaks down cyber losses in 10 categories, you know, broken down, such as information privacy, proprietary data loss, business interruption, and it goes on, including reputational damage and fraud. And for each of these categories, we break down basically what are the loss components? They make up each gonna say category. So for let's say information privacy, you need to account for losses related to spending time responding to an event where there may be a loss of data and then management of that process. You know you need to account for PCI liability or information privacy liability or regulatory reliability. So having a model like this is really important for companies, because oftentimes at a moment of an incident, they do not know how to account for the potential cyber losses. They do not know what cost categories can be involved. They may have a high level understanding, a superficial understanding, to the point where even in a recent hack, you know, with United Healthcare, we had the CEO report to Congress, and they estimated the total losses to the recent hack they suffered, you know, through ransomware, to $1.6 billion at the institute level. You know, with the support of the, you know, major underwriter, which I'm the president of Safe Security, we estimated those losses to be potentially double that. And the reason for that is that the company did not have a model like

FAIR MAM, and is not able to account for all possible can I say losses, including things that happen as a result of a fallout, you know, that happened more later in time, not to the moment of incident, things like as data breach notification, dark web monitoring and litigation cost, These can reach hundreds of millions of dollars for company of size, United Healthcare, and it would not accounted in the telling of the losses that the CEO presented to Congress. So we actually estimated those losses to be double that, potentially up to $3 billion and we made that public for companies who want to see how. So a model like FAIR MAM can assess public hacks. You can go to a website called how material is that hack.org and you'll find the public disclosure of our estimation of those losses using the Standard Model FAIR MAM,

[Rachael Johnson]
We do a quarterly risk survey as part of our global economic condition survey of each quarter. And since we've been doing the what your organization's top risk priorities, cyber is the only one since the last quarter of 2022 that's been in the top three consecutively every quarter. But then we also have an open ended question that it says, What do you feel is the most underestimated risk at your organization? And 90% of the time, those are related to cyber but I'll tell you, a lot of our members tell me that they are really struggling with getting the buy in that they need. So you know how they can explain that ignoring it is more costly than defending against attacks themselves. It's not a matter of if it's not a likelihood it's when. So I just wondered, you know, with all these cases and they're happening more and more often, what you think accountancy professionals can learn from them, especially with most organizations saying they're already in risk overload and thinning capacity mode

[Nick Sanna]
Yeah, I think the way they can provide a valued organization is to partner with the head of information security and tell them, let them know that standards model for accounting or cyber losses exist. You can actually quantify risk in financial terms, and that makes it going to say allows the proper oversight and governance to happen, because if you can put $1 sign next to possible losses you're going to experience, the business kind of can intervene and tell you, we can live with that, or that's completely unacceptable it's beyond our tolerance level, and we need to mitigate it. And then the CISO can provide options mitigation option, and jointly the organization can decide how much risk is acceptable and how much is not and how much investment is necessary or not. Those are business decisions. Those are decisions where accountants and by quantifying cyber risk can really help the organization make those smarter decisions. And that's very important in healthcare, where oftentimes these organizations are run by people that have a medical background and do not have an IT background, a medical or business background, and so being able to translate the impact of cyber risk in business terms, in financial terms, allows them to be part of the decision making, and allows them to make the decision they need to make, on how much risk is acceptable, how much not, and how much to invest or not. That is not a CISO decision. The CISO is there to provide options. And I think this is exacerbated in healthcare, because a lot of organization healthcare delegate or outsource their processes and their IT processes to third parties, and they also heavy users or third party applications like, you know, Cerner is a big application in the medical field, you know, or Epic, and many organizations use those applications, and they have no idea of the security setting of those applications and how much exposure they have to those application and those third party processes. So being able to have a clear understanding of the risk exposure to the usage of those application, the user of third parties, and how we're using IT System internally is very important for the business to make the right decisions. Otherwise, you're going to be completely reactive mode, just reacting to incidents after happen. You need to be proactive, but you can only do that when you look at the problem in the eye and then proactively decide how much you want to mitigate it, how much you want to invest in dealing with it, and that is not possible without a financial model like FAIR, which is currently the only standard quantification model out there. Otherwise you're left guessing, and you're basically managing risk by going from crisis to crisis.

[Rachael Johnson]

And it's hard not to bring up AI in that respect too, because it's just lightning speed exacerbating everything, and, you know, helping the attackers launch more sophisticated attacks. Indeed, it would be really great if you could describe, of course, there are many, many good things happening. There's good and bad things for AI and particularly in the healthcare sector, as a prime example, with early detection of diseases. But also, like you said earlier, with all the data that the concentration of data, and many of our members admit in healthcare they don't know where they're stored or where things are located and so on. So it would be great if you could just talk a little bit about how organizations can actually use AI to detect and respond to attacks more quickly.

[Nick Sanna]
Now, yeah, now I can give you the example of FAIR Security. Again, I'm a president of FAIR Security full disclosure there, and we apply the FAIR Standard and we are heavy user of AI because most of our customers are telling us that they are the in the cyber practices that make a heavy use of questionnaires to understand the state of affairs both internal parties, and that's a very manual endeavor. They spend more time managing questionaires and manual processes and actually are doing fixing security. So we applying AI in many ways. Just a simple way of doing it is basically using AI to interpreting the responses from third parties to the questionnaires so you can understand the state of controls automatically and calculate risk off it automatically using a standard like FAIR. So in a platform like, let's say, if it's really AI driven cyber risk communication, where you can interpret the data feeds from the third party, the responses to questionnaires, you can interpret, kind of, say, the readings of your own system using AI, where the interpretation is done by the machine, and AI is also helping you, providing recommendation on what to fix. What are the controls that are most effective in reducing either the probability or the impact of an event, and that replaces work that typically could be done by human beings that would take many, many hours, many days and months, if the machine can take care of that automatically, you basically spending most of your time then managing the problem, managing risk, versus managing the process, which has been the case now, which is sending questionnaires, fetching the data, trying to make sense of it, and never having enough time to actually fix the problem, reducing risk. So I think AI, the use of AI from in applications like Safe, allows you to change the equation, invert the pyramid, spending much less time fetching the data and interpreting it, and more time actually fixing, you know, or improving controls.

[Rachael Johnson]
Yeah, good advice, and I do see that too. Just talking to ACCA members in the healthcare sector, just about a lot of questionnaires, a lot of kind of overlaps and wasted things aren't really developing any metrics or any use for them. So I think, you know, there is a lot of stepping back and assessing to be done. I just thought it would be great to end about, you know, just that any nuances compared, you know, in terms of giving advice about all this, any nuances compared with other sectors?

[Nick Sanna]
Yeah, I think that health care, I think, has the confluence of two things. One is that typically, a health organization don't have very vast cyber security teams, and they typically probably spending less than a financial institution would do traditionally, because they're in a different type of business, and they put more emphasis on investing in new applications to provide better care, of course, and less in security was an afterthought for a while. I think it is catching up, but it's still a lot more work to be done, and they are run by professionals, mostly, you know, the medical professionals, and so they need to understand that there needs to be a translation mechanism that tells them how severe the problem is and what they can do about it. So it's a sector that requires more help in doing that, and so models like FAIR, application, like Safe provide that aid in giving automated ways to understand your loss, export, what to do about it. The second thing I would mention here is that healthcare organization typically outsource a lot. We spoke about a bit earlier, but they probably outsource more than other sectors their it because it's not their core expertise. So they outsource, you know, the use of applications. They subscribe to medical kind of application developed by third parties. They outsource a lot of the IT, management and

monitoring. That means also the attack surface is not limited just to the internal system. It needs to include also the system the third parties. So they cannot just think about cybersecurity in the confines of the service they manage. They need also think about the application and the services and the they are run by their third parties. They need to being able to look at cybers from a holistic perspective, because ultimately the regulator is going to hold them accountable. Whether you have an outage that is, you know, happening on your internal system or driven by a third party, they're still liable. And so we see many companies, they see these two aspect managed by internal security and my third party security as in a disjoint way, in a separate way. They need to be managed as one because it's one attack surface. It's one way of delivering service to and security to your customers and patients, and they need to manage accordingly. So my advice there is, don't look at these two things separate. Look at your attack surface as one, it includes both your first party systems and your third party systems. And so you need to find security measure, security management and risk management practice that encompasses both.

[Rachael Johnson]
That's so great. Thanks so much for coming and talking with us today. I know this will be really valuable advice for members from all sectors where they can learn more. I think it's an ongoing learning process. So we look forward to having you back again.

[Nick Sanna]
Thank you for having me again. The old adject says, you know, you cannot manage what you don't measure, so the accountant has a big role to play, and the model like FAIR can help greatly.

[Rachael Johnson]
Stay tuned for more episodes related to enhancing risk management in the healthcare sector. These episodes will supplement our upcoming report, which is part of a series of thought leadership pieces exploring approaches to risk management across different industries.

ACCA professional Insights Team, seek answers to the big issues affecting finance professionals. Find our latest research at ACCA global.com forward slash professional insights.

This podcast was brought to you by ACCA. Find out how we think ahead at ACCA global.com