THINKING the UNTHINKABLE

Thinking the Unthinkable | Podcast

Jargon Jailbreak! Unthinkable Risks That Cost Trillions

Guest Speaker **RYAN DODD**

“We can't wait, right? Attacks are going up year on year. Every year, there's another crisis, and it's not going to be the big, huge event that takes the whole world down.

It's very easy to get distracted by talking about this event that may or may not happen. It's these billion dollar hits to critical infrastructure, hospitals, and that are impacting people's lives and costing money right now. The attritional losses are the ones that we need to be looking at and taking care of, and stop talking about this.

You know, some cyber event in the future that's going to take the whole world down. It's easy to get distracted with that and not focus on the here and now which we need to deal with.”

Nik Gowing
Welcome to talking about Thinking the Unthinkable, our latest leadership conversation and podcast. Hello. I'm Nik Gowing, Founder and Director of the Thinking the Unthinkable project since 2014.

How vulnerable do you believe your organization is to massively destructive cyber attacks? The unthinkable is that you're not even at first base when it comes to realizing the scale of risk. You probably believe your risk manager and the cyber engineers who speak a techie jargon you don't even understand have got it all covered, but that's not really the case. Cyber is an existential threat like sustainability, so we want to shake you.

Joining me from Barcelona is Ryan Dodd. He spent 20 years in financial markets. He came to the insurance business as an outsider. He's now Founder and Chief Executive of Intangic, which describes itself as a cyber risk validation company. Intangic continuously validates the size, the cost, and structure of large organization cyber insurance programs.

But I watched and heard Ryan shake an audience of insurance and risk managers and realized Thinking the Unthinkable loyalists like you need to hear his stark message and the scale of vulnerability that we all face. Welcome, Ryan.

Think Unthinkable Ltd is based in London and incorporated in England and Wales.
Registered Office: 115c Milton Road, Cambridge CB4 1WE, U.K.
VAT No. 254114435. Company No. 10842200

contact@thinkunthink.org
thinkunthink.org

Ryan Dodd
Thank you.

Nik Gowing
What's the scale of cyber risk we're all facing. You said a lot of money is spent building walls, but the hackers just walk through the front door.

Ryan Dodd
Yeah. So I think one of the things that people need to understand is sort of how much technology pervades everything you do, all day, your work day with your children, and think about how much technology is driving the value of all the companies that exist now that are part of our lives.

And then consider the following statistic: that in the insurance market, the whole property and casualty insurance market globally, only 2% of that is covered by cyber insurance. Meaning, even though the stock market value is probably about 90% technology, the insurance market that underwrites that risk is only 2%. So there's an enormous mismatch.

And I could give you all sorts of numbers that could explain that, but I think ultimately you need to remember that the gap between how much value is at risk and even how much is lost every year due to technology losses, hyper risks, is trillions of dollars larger than the amount of money that risk is covered. There's just no other industry like it.

If you look at the gap between property for storms, climate change, weather fires, it's not even close. The ratio between how much is covered and how much is at risk, and how much is lost, is much, much, much smaller. So I don't really think people understand that this gap is as large as it is and it's growing.

So that's a good example in numbers terms of how far or how overconfident we are that there's not going to be any cyber hacking, even though, again, that's pretty ridiculous, but the numbers would say we're really confident there's not going to be a problem.

Nik Gowing
So what are you confronting at the moment, Ryan, from leaders and executives? Is it complacency? Is it denial? Is it ignorance? Is it fear? Because nothing of what you're saying should really be unthinkable, given where we are.

Ryan Dodd
True.

Nik Gowing
...these days.

Ryan Dodd
I think it's driven by two things, both very human emotions. One is that with an issue like technology risk, most of us, including corporate leaders, believe that everything is under control. They're doing a great job because it's an invisible risk and you don't really see it. So, unlike wind or fire or health, you don't see that it's happening to you. So, I think there's, on the one side, significant overconfidence. That leads to the belief that maybe we shouldn't spend the money we need to spend to protect against the unthinkable.

And I think that you have a situation where the fear that's coming is being spent on more protection, right? Let's spend on protection, protection, protection. And I think the overconfidence is the reason why they're not spending it on what they should be in addition, which is when your protections don't work, how are you going to get up the next day when things go wrong and have the resources to get back on your feet and, more importantly, protect your customers who are now at risk.

And you look at hospitals that have been breached, you've looked at, you know, whether it's medical devices, people's private information, supply chains with critical infrastructure. So, it's those two emotions: overconfidence—I don't want to say arrogance because it's a pretty human emotion to believe that you're confident—combined with the sort of fear of not believing we can spend on protection, that is leading to where we are now. I mean, there's just not a belief that things can go wrong, despite evidence showing that the number of breaches is increasing year on year, over 100%.

Nik Gowing
I was very struck, though, Ryan, when I heard you speak, when you talked about the high priests of cyber speaking in a very strange language, and no one understands what they're talking about. Yeah. What does that mean? What does that signify? Does it suggest a big disconnect?

Ryan Dodd
I think that it, I think that, like, there are certain industries, finance is one of them. And I, you know, spent two decades in the finance industry, and I think insurance is part of that, is similar to cyber. And this is you speak a language that is meant to scare off others who want to challenge your authority, and you want to believe that you, and only you, have the understanding of this mysterious, invisible force that will impact others.

And that's why I use the term High Priest speaking Latin, because ultimately, it's a way to preserve authority. But the problem is, it's causing people in this area to be siloed off. And so the technology, even though it's running through everything in our lives and all aspects of our business, you and I are interacting right now through technology, it's, in fact, being treated from a risk perspective and a risk management perspective as a separate, siloed entity that is somehow separate from everything else. And speaking in this language preserves the authority of those managing it, but it also is causing the rift or the lack of communication between those that should be communicating

with the cyber protection people and those that are also managing the business, including the risks. Believe it or not.

Nik Gowing
There are risk managers in so many corporations, large, medium, and small. Surely, they are the people who one should have confidence in, or are they actually belittled and marginalized and not thanked for anything?

Ryan Dodd
Yes, I think that they have a very thankless job. Ultimately, the world is very complex, and it's getting more complex. And I also think that part of what you're seeing now is we've been undervaluing and underpaying for risk for years and years and years, and you're seeing that across all insurance lines and...

Nik Gowing
But shouldn't risk managers sort of raise their head, raise their hand, raise alarm bells? Are you saying...

Ryan Dodd
They...

Nik Gowing
That they don't want to?

Ryan Dodd
They do. The problem is they're seen as a cost center. You never make profit if you're buying insurance. So they're constantly fighting the growth teams that get the money and the budget to make the next quarter's earnings. And so the risk manager has to find ways, and they do find ways, across multiple risk lines and insurance lines to optimize that budget to prove their worth in dollar terms. And that's really how they have succeeded across sort of the traditional risks.

Now, cyber is new, and so you do have a group of risk managers who are thinking differently moving forward, but the vast majority are still saying, I've just now got my head around the climate risks, and now I've got to deal with this human behavioral risk from these very talented hackers who are creating chaos. So it's somewhat a challenge. Let's put it that way, right. They're covering so many things, but they're now having to catch up very quickly to a human behavioral risk that shifts very, very fast.

Nik Gowing
What kind of status and standing do they tend to have inside companies? Are they, do they have board positions?

Ryan Dodd
Well again, because they are often a cost center, they're only called upon when a disaster has happened. So oftentimes it's a bad sign when the risk manager has to talk to the board; it means something has gone wrong. But in fact, no, in my opinion, they don't have the status they should have in many organizations, and they certainly, when it comes to technology, don't have the authority to speak at the same level as other division heads, because they've just traditionally been seen as the insurance person, not someone who's managing or working with the cyber team to manage this.

And so I think it's a big issue, but I think it stems from traditionally, risk is a loss leader, right? You're spending money, you're not seen as delivering value to the organization. So there's a mindset change that has to also occur.

Nik Gowing
What do you think the willingness is of the C-suite, the Chief Executive, the CFO, the COO, and others at that level, of those coming up, to realise what the kind of thing you're saying here, Ryan?

Ryan Dodd
Well, I wish I could tell you what I want, but I'll tell you what is actually happening. So here's what I see, Nik. You see that cyber is always number one, two, or three in terms of top corporate risks they're worried about. So they're worried about it, they're fearful of it, but they continue to spend money on protection and just hope it goes away.

I think that you're just now starting to see, because of the number of attacks that have happened, the executives are getting pushback from shareholders and from the board and stakeholders to stop pretending like this is not going to happen and start putting a program in place, even if it costs money, for after it happens. What are we going to do after it happens? How are we going to get back on our feet after it happens?

So I would say that the numbers right now, and I think they will continue for months or years, would suggest that given the choice, they're spending it on protection, not on insurance, meaning not on recovery and crisis. But that is slowly starting to shift, but it has to go so far the other way until it sort of balances out relative to other risks. So just now seeing the first signs of change.

Nik Gowing
Now you've actually used one word, Dick, D, I, C, K, for four ambitions that everyone should have. What are they? Just briefly explain them to us in the key words, which are there?

Ryan Dodd
Well, the first thing was, I wanted to make sure that was memorable. So thank you. You've got to keep the insurance industry on its toes. You know, it gets a little complacent, so the first one is detection, right? And what I mean by this is that if you're really thinking about your risks with cyber, you've got to have someone else independently looking at your network outside of your inner circle

and your inner sanctum. If you're inside the castle, you're not seeing who's outside attacking it, so detecting who's out there, early warning before it happens. That's the first thing. It's really important because that lowers that self-confidence that often leads you to being attacked.

Second thing is you really need to integrate, and it was really important. You've got to integrate your risk officer and your risk team with your cyber team. I have talked about this time and time again, and it's really important that those two members, or those two teams talk more than once a year. Right now, they talk once a year when it's time to buy insurance. They need to be talking all the time, and they need to be seen as the same team.

The second one was controls. And I talked about this and it's something...

Nik Gowing
The third one.

Ryan Dodd
Yeah, the third one is controls. And why is that so important? Because cyber is a human behavioral risk that's trying to be detected or dealt with in an industry that is used to having actuarial data sets that go back decades. So cyber controls are the most visible example of the insurance industry saying, "This is the cause of hacks. Everyone needs to buy all these new controls and hacking will be stopped." Well, hackers figured out very quickly how to get around those controls as soon as they were put in place. So there's a constant arms race. And I think I use this point to say controls are important, but they're not everything, so don't be too confident in your controls because they can also be walked right around.

And the last one was know, and that is, know your enemy. And it goes back to one of the points I was making time and time again, that because cyber is looked at from an insurance perspective, from the question of, "What do we know about ourselves?" Well, what we know about ourselves is all the information we have inside the palace gates or the castle gates, right? What's not done enough of is monitoring the attacks that are happening outside, not just to you, but to everyone else. If you can see how targeted we are as an organization versus everyone else, and monitor that, and what types of activities the attackers are doing, that gives you a pre-warning that you need in order to put those resources in place that can avoid the bigger breach.

And there hasn't yet been enough emphasis on that in cyber. What's interesting, I think, is that it's something that we use almost automatically in other risk perils, like workplace incidents. We all know that the number of slips and falls ultimately leads to larger workplace injuries. It's true across every industry. It's true with bad drivers. It's true with health insurance, right? So trying to show that as you observe the peril, as you observe the behavior of the attackers across a large scale, that's going to give you a much better insight into when to take action.

So I did that acronym sort of tongue-in-cheek, but I wanted it to be memorable.

Nik Gowing
Remember D.I.C.K.

Ryan Dodd
Yes.

Nik Gowing
D.I.C.K, Ryan Dodd, okay. Well, look, we've got a couple of minutes left to crystallize the alert. We're talking about unthinkables, which actually is thinking the unpalatable as well. And what you're talking about is unpalatable. It's inevitable. The scale is dramatically increasing, by multi, by 10x, 5x, 6x. It's dramatically changing. What is your message to those who are saying, "Is he overstating it?"

Ryan Dodd
No, I'm not. A positive message would be there are ways to start to close this coverage gap that don't involve just buying insurance blindly. A lot of the things I spoke about was prevention, detection, taking steps to do that. But that's not enough. Nik, and I can't express this enough, there is still very much an attitude in the people who are producing the software and the hardware that lead to vulnerabilities through which attackers exploit their victims. They're no longer, and they never have been, responsible for those vulnerabilities. And so if that industry can create buggy software that gives opening for attackers and the hardware companies aren't responsible for the hardware they're putting out there with vulnerabilities, this is going to be a tough challenge to take place. So until...

Nik Gowing
Let me just ask you, what about, finally, the mindset of people you're dealing with about what they've got to change dramatically.

Ryan Dodd
They're going to have to change their view of what risk really costs, and they've got to really understand that if they want to enjoy the upside and the positive profits from technology and the productivity, they've got to also invest in protecting the downside. Because that gap is becoming absolutely unpalatable, as you put it, it's here. We can't wait, right? Attacks are going up year on year, every year there's another crisis, and it's not going to be the big, huge event that takes the whole world down.

It's very easy to get distracted by talking about this event that may or may not happen. It's these billion-dollar hits to critical infrastructure, hospitals, and that are impacting people's lives and costing money right now. The attritional losses are the ones that we need to be looking at and taking care of, and stop talking about this. You know, some cyber event in the future that's going to take the whole world down. It's easy to get distracted with that and not focused on the here and now, which we need to deal with.

Nik Gowing
Ryan, thanks so much. Our time is up, sadly. You can reference every detail that Ryan has given us. A transcript of the podcast is posted in parallel on our website, along with contact details for us and for Ryan. Do please join us when we next have a conversation about thinking the unthinkable.

From me, Nik Gowing, until the next time, keep thinking unthinkables. More than ever, it's both possible and necessary, as we've just heard from Ryan. Thank you for joining us, Ryan.

Ryan Dodd
Thank you very much.

Nik Gowing
Bye. Bye.

Ryan Dodd
Thank you.