**Rapid Response Transcript – Bipul Sinha**

**"'We have an all-out cyber war right now.'"**

**Click here to listen to the full Masters of Scale: Rapid Response episode with Bipul Sinha.**

> **BIPUL SINHA:** We have an all-out cyber war right now. Accelerated digitization has really exposed a soft underbelly for cyber attacks.
>
> We are seeing this independent hacker groups are aligning with nation estates. The technology underpinning Russia is strong.
>
> A country with technical underpinning and knowhow can use this power for disruption. What's the weapon? And the weapon is speed and paranoia.
>
> Even when you don't make a statement, even when you don't explicitly support a cause, you are a target.
>
> I think the game has changed. You now have to have a way to prepare and respond to the attack that will inevitably come to you. You don't want bad things to get in, but if they at all get in, then you have a way to respond and contain damage and not let it become a huge problem.
>
> Every kind of attack on every infrastructure is fair game. And at some level, the disruption that these attacks cause is immaterial whether the source is state-sponsored or individuals or groups. So the question is: how does a business or a government deal with it?

**BOB SAFIAN:** That's Bipul Sinha, co-founder and CEO of cybersecurity firm Rubrik.

Rubrik has more than 2500 clients around the world, from corporations like The Home Depot and Estee Lauder, to national and local governments.

I'm Bob Safian, former editor of Fast Company, founder of The Flux Group, and host of Masters of Scale: Rapid Response.

I wanted to talk to Bipul because, with Russia's invasion of Ukraine, cyber risk has dramatically escalated.

Bipul explains why state-sponsored actors and cybercriminals are both heightened threats, and how traditional cybersecurity approaches are adjusting to counter them.

He describes a complex ecosystem in which economic sanctions actually encourage malicious players.

He also points out what we can do to protect ourselves from basic cyber hygiene to recovery strategies.

Espionage, infrastructure disruption, and misinformation are all inevitable, he says.

We need to build appropriate habits to keep Russian hackers and other bad actors at bay.

**[THEME MUSIC]**

**SAFIAN:** I'm Bob Safian, and I'm here with Bipul Sinha, CEO of Rubric. Bipul, thanks for joining us.

> **SINHA:** It's my pleasure, Bob. Thank you so much.

**SAFIAN:** So with Russia's invasion of Ukraine, there's been heightened discussion of cyber risks, cyber war even. You head a cyber security firm. Many of our listeners are not cyber experts, though they're dependent on digital connectivity and tools. I'm hopeful you can act as our guide, giving us a framework for understanding the cyber landscape, where things are today, what's changed or changing the risks, steps we all might take in response. To start things off, perhaps you can clarify for us who are the main players or groups of players that we should be aware of. I mean, there are individual hackers and state-sponsored groups and murky sounding networks and financial scammers and governments themselves, how should we think about that landscape?

> **SINHA:** First of all, the Russian invasion of Ukraine is tragic. And our thoughts and prayers are with everyone who is impacted. And as you know, when you have, like, a land war or pandemic, these are the kind of like black swan events that don't start a new trend, they accelerate an existing trend. So if you think about the actors involved in this equation, you have state-sponsored elements. You have bored people in their basement trying to show a middle finger to corporations for fun. Then you have actual cyber criminals who are actually raising capital for their nefarious activities. And then finally you have a set of actors who are in solidarity, either with oppression or oppressed, trying to show their power and align themselves with one of the aggressors on the other end. So if you see the recent news, Quanti Group came out in support of Russia openly. Anonymous Group came out supporting Ukraine and trying to kind of expose Quanti Groups' sensitive content. So we have an all out cyber war right now.

**SAFIAN:** So when you talk about the cyber war that's underway, can you give us the lay of the land of the different kinds of attacks that are out there? Because we hear about malware and ransomware and denial of service attacks and data breaches. And maybe you could just clarify for us sort of what those main groupings are, or are they changing all the time?

**SINHA:** So if you think about the components of cyber warfare, they are really kind of three high level broad categories that these things fall into. So you have espionage and critical technology access or stealing, however you define it. So this is purely for nation-state advantage to get the know-how to understand the planning of the other side and have access to critical technology.

The second piece is infrastructure disruption. Be it supply chain, energy infrastructure, anything that can have significant economic ramification, how do you disrupt that infrastructure? And finally, the third piece that has emerged in the last seven to 10 years is the misinformation campaign to manipulate public sentiment. Because both for the aggressor and also the impacted parties, they're trying to build momentum for public support.

So you have these different interests. And what is also interesting is that in the modern era, any kind of aggression comes with swift response with respect to sanctions. Then the cyber becomes an even bigger part of the geopolitical considerations because banking and finance infrastructure, as you know, is the most globalized infrastructure. And if somebody's thrown out of their infrastructure by a sanction, that encourages these individuals and groups to start raising capital by keeping hostage your data, your application, your infrastructure.

**SAFIAN:** So by putting sanctions on Russia and making it more difficult for players in Russia to access capital, that may encourage more of the kind of ransomware and financially-oriented cyber attacks that could be accelerated by this?

**SINHA:** Exactly. And this may not be the state that is directly involved. Some people use this as an excuse to accelerate or elevate their attacks. The accelerated digitization to have more productivity in liberal democracies has really exposed a soft underbelly for cyber attacks. So the more digital we become, the more digital products and services that we use in our personal and professional life, it has a direct impact into increased surface area of attack. And it is exposing a soft underbelly, as I said it, to the attacker. So now you have the impact of financial infrastructure and banking infrastructure not being able to participate. And you combine that with this soft underbelly because we are open societies, open transactions, which opens up this infrastructure for attack.

**SAFIAN:** I saw news that Toyota had to halt its factory production for a day recently due to a cyber attack. And this was just after Japan had expressed some support for Ukraine, and there's speculation that maybe it's connected. Do we know if it's connected or not?

**SINHA:** See, the thing with cyber is when there is a doubt, there is no doubt. So if you feel like the attack is happening for a certain reason, there is always some truth to it. And the situation is that every organization, whether it's a business or government, really needs to think through the cyber implications. Even when you don't make a statement, even when you don't explicitly support a cause, since you are an important part of the economic infrastructure, you are a target. We are seeing independent hacker groups aligning with nation-states. So every business or government has to really ensure the safety against malicious insiders as well as planned cyber attacks because these groups are not limited to outside attack, but they also could recruit insiders for malicious activities.

**SAFIAN:** Insiders within your organization?

**SINHA:** Exactly.

**SAFIAN:** We've heard some people say that Russian cyber capabilities are on a par with the U.S. How do we know that?

**SINHA:** The technology underpinning Russia is strong. And given the cost of software development, and again, this kind of bad software and also software development, has come down. And with the ubiquitous cloud infrastructure, things like that, it's become easy to build and test and write code. So as a result, a country with technical underpinning and know-how, combine that with the ever lower cost of software development, it has created a unique situation that you can use this power for goodness, by creating tools and technology for betterment of human being, or you can also use this power for disruption.

And in some ways as Americans, what used to be the case 20-30 years ago, where we had significant know-how, in relatively isolated scenarios we were developing technologies and had unique points of view, in some ways the internet and mobile platform has leveled that know-how. So the question is that in this scenario where the knowledge is proliferated, technology underpinning exists in multiple countries, what's the weapon? And the weapon is, or the unique advantage is speed and paranoia. And that's the thing that every business and government has to think about. How do I enable an open system, low transaction cost, high transaction governance, while ensuring safety? And these are opposing values, but we have to find harmony. We can't swing one way or the other.

**SAFIAN:** So for the governments and corporations, and NGOs that are actively isolating Russia or assisting Ukraine, they may be particularly in the crosshairs as targets right now. Are there different ways you try to prepare, or walk that line that you're describing for state sponsored risk, than you would for other malware and ransomware attacks? Does it matter if your computing environment is more cloud-based or on-premises? How do you react differently if you find that you are maybe facing this heightened risk now?

**SINHA:** Every kind of attack on every infrastructure is fair game. And at some level, the disruption that these attacks cause is immaterial whether the source of disruption is state-sponsored or individuals or groups. So the question is how does a business or a government deal with it?

If you look at traditional cyber security, it has been very focused on prevention, detection, and investigation. I think the game has changed. The game is not only about infrastructural security, but also you need to have data security. Because all of the infrastructure security is really protecting your core IP, which is your data. So you now have to have a way to prepare and respond to the attack that will inevitably come to you. Because even if one in one million things pass through, you need to be ready to respond. So the real game is: How do you compliment the infrastructure security with data security, particularly around data resilience, data observability, and data recovery? You don't want bad things to get in, but if they at all get in, then you have a way to respond and contain damage and not let it become a huge problem.

**SAFIAN:** I talked with the CEO of SolarWinds for this show last fall — SolarWinds, a victim and a conduit for a sophisticated interruption. And his advice was mostly about fishing and basic cyber hygiene. Two-factor authentication and things like that. The feeling might be that efforts like that are just for nuisance level threats, or is the same gateway that's exploited for those kinds of things exploited for more dangerous intrusions? Small holes and small players lead to big impact, or is there a hierarchy of where your risk is, and where you put your attention?

**SINHA:** If you look at the history, the beginning of all big, great things have been small. And if you have a chink in your armor in terms of people's habit, or two-factor authentication, or basic hygiene, you have a huge hole at a very low-level of sophistication. And in some ways, if you don't fill that hole, it becomes a huge problem.

The way to think about this is the following. With the internet and with mobile computing, think about everyone living on a freeway. So any car passing on freeway, that car can come from anywhere, can get into your house. So you need to have basic hygiene of closing your windows and doors and prevent things from getting in. You can't have everything open when you live directly on a freeway.

At the same time, you need to have a strategy to recover, should anything come in. Somebody breaks your door, and then you need to have a recovery strategy — the shield that lives around my crown jewel. So you need to have this thinking around hygiene and basic things covered. Then assume that things will still get in. How do you provide resiliency, observability, and recovery. And bringing this whole thing together is: you need to have a real strategy. You can't, like, piecemeal this, or miss an important piece, even on the lower value chain or the highest sophistication.

**SAFIAN:** Before the break we heard Rubrik CEO Bipul Sinha outline how cyberwar is unfolding in the wake of Russia’s invasion of Ukraine.

Now he talks about what he calls the cat and mouse game between hackers and security experts, and the complex ecosystems on both sides of that equation.

He also explains why an open market system is, by its nature, vulnerable to attack, but says that doesn't mean we should lose hope. By working together, he says, the threats can be contained.

You used the word inevitably a little earlier. It sounds like it's not really possible to stop the infiltrations with the sophistication of bad actors. It's going to come.

> **SINHA:** The war is not about technology. War is about social engineering and psychology. They are playing with your system one. You come into work, you log-in, you get a message, and before your system two can really process what this is about, you do a click, and you are infected. So the attacks are not just technical. Attacks are playing with our emotions and our hidden brain, our system one as Daniel Kahneman said it. And that's where the game is.

**SAFIAN:** In the Hollywood version of hackers, it seemed like they almost have these supernatural abilities, geniuses who can get into anything in a snap and control anything remotely. That's not real.

> **SINHA:** They're trying to map their expertise into human emotions. So they know that people might put the password as their kid's name, or birthday human emotions, human laziness, inherent laziness when we set the password, they try to exploit that. It's not that they're coming up with the actual password out of thin air. They're mapping their technical understanding with human understanding. So in some ways it's true, in some ways it is not. But irrespective, unless you have the basic hygiene covered, unless you do things with a paranoid mind, and prepare for the worst case, and have the strategy and operational chops to recover, you are in danger.

**SAFIAN:** You noted this earlier. Even before the Ukraine invasion, 2022 was shaping up to be an eventful year in cyber. There was a joint report from the U.S., UK, and Australia cyber defense agencies that noted that ransomware was on the rise. We saw that even the NFL's San Francisco 49ers announced they'd been victims of ransomware. Is going public when you're attacked a good idea?

> **SINHA:** We can debate whether going public is a good or bad idea. From the organization perspective, by putting themselves out there that we had an attack, it means that somewhere we slipped up, is a hard acceptance. But if you look at the society as a whole, we benefit from this information, because now we can harden at least known issues that companies face. So they at least know the issues that companies face. So there is a balance, and we need to ensure that the individual cost is reduced upon such a disclosure and societal benefit is maximized.

Having said all of that, I personally believe that this is a cat-and-mouse game, and folks have fundamentally understood that there's a way to raise money or earn money by hacking. So just like we come to work and do our job in the office, folks in North Korea are maybe going to work in coats and suits and ties for hacking for raising capital. And in that scenario, you cannot stop this. If you close one loop, they will find something else. Because as long as the software gets developed, surface area increases, somebody makes a mistake, something will happen.

We have to assume that worse things will happen, and how do we prepare for the worst, and make sure that the damage is limited and we are able to recover.

**SAFIAN:** When you talk about this cat-and-mouse game, how much do cyber defense firms like yours collaborate with each other? I mean, you're competing in the marketplace, but at the same time, you kind of need each other to share what you're seeing or what you know is working to be able to stay ahead of the bad actors who are trying to come in.

**SINHA:** Exactly. Nobody lives in isolation. What we are delivering is data security. Our partners are delivering infrastructure security. And those two things have to come together. The whole cyber community is part of an ecosystem where we have to collaborate and compete, as well, for the business. But the market is very large. This challenge is huge. No one company can solve it. So it's better to be part of the ecosystem and collectively go make it happen.

**SAFIAN:** Are there lots of sort of back channel conversations that you have with other firms about, hey, we've just seen this, or we've just caught that, or are you seeing things like this in your networks, so you can understand whether something is more isolated or whether it's part of a broader reach across different organizations?

**SINHA:** There is back-channel chatter, but also you have to understand that we live in a competitive capitalist economy, and if some company finds a unique problem and a unique solution, they want to monetize it and create market traction. So it's all about the balance between societal benefit and individual business benefit, and folks are trying to find a balance.

**SAFIAN:** And I guess that's another opportunity that bad players can take advantage of, because there may be some places that are not as secure, and therefore you can go and try to attack those areas.

**SINHA:** The bad actors are always trying to find an angle to attack. Nation-states have also started to accumulate strength just like strategic weaponry or tactical weaponry, the cyber is also a weapon that you can potentially unleash. So now there is a marketplace where there's a know-how. Nation-state wants to have their own control on that information, because that's an IP or a weapon that they can use. Businesses are trying to solve that problem as a cyber firm for the rest of the businesses and government. And then independent hacker groups are getting into action because they have both a monetizable source of money as well as name and fame for themselves. So it's a very complex ecosystem.

**SAFIAN:** Yeah, it is. It's a whole ecosystem. And I think a lot of businesses used to think that, “I only have to worry about this at a surface level because the government is protecting me from bad things that could come on a more systematic level.” And if I'm hearing you, you can't necessarily rely on that. Whatever the government is doing, you have to protect yourself also.

**SINHA:** Nobody can give you a foolproof umbrella. So you get some safety nets, some security umbrella, from the government, but you can't lapse on your own security. It's like you live in a city, the police are giving you a security umbrella, but you have to be situationally aware if you're walking out in the middle of the night. So you have to do both.

Don't trust anything that you have not verified or not authenticated. There has to be a minimal level of authentication before you enter into any kind of business transaction, access of systems and data, physical, virtual, all sorts of things require a minimum level of authentication and trust. And all of us have to, when we see content, when we see any activities, we need to look at the origins. We need to verify it. We need to have a way to offline ensure that it is real if we are doubtful. Again, we cannot not take action because our business and our world depends upon this kind of trust communication, but then the bad guys are taking advantage of that trust. So instead of implicit trust, you want zero trust.

**SAFIAN:** Yeah, no, that line between zero trust and openness, which is another goal we have. As you say, it's a paradox because we need both, but they are in conflict with each other.

**SINHA:** You can't build a capitalist society if everybody's so tight about trusting and not sharing. Otherwise your cost of transaction goes significantly high. If you look at our legal framework in our country here in America, if you look at the transactional governance and enforcement of contracts, these are built to reduce the transactional cost so that you can bring more players into the marketplace and have a more liquid market. But security concerns increase that cost. And so the balance that we have to establish, at what point that cost outweighs the liquidity in the marketplace? So we have to be ever vigilant and all of us have to do our own part to make sure that we do the basic hygiene to keep the cost low enough so that we can have high liquidity, a very nice functioning marketplace, more participants, while we ensure safety and security.

**SAFIAN:** The heightened cyber risk right now, how much more concerned should we be, or are you, than you were a few weeks ago before the invasion happened?

**SINHA:** Ransomware and data security threat is the biggest challenge to our economy. This really started with pandemic because pandemic really accelerated digital transactions. And when you have so many digital transactions, you increase the opportunity for attacks. And these trends don't reverse just because the pandemic risk has reduced. Doesn't mean that the digital transactions are diminishing. And so we are already living in an atmosphere where there is a heightened cybersecurity issue, because it's a very target rich environment. And if you combine that with this geopolitical land war scenario, now you have more actors motivated around this theme.

And so you have really created another step up and accelerated this trend. I think this will continue for a while. As long as we have digital interactions, digital experiences, and digital business, this problem is going to continue. And that's where we need to establish the balance of safety and enablement.

**SAFIAN:** Yeah. As you talk about it, I could get anxious about it. Are there things that make you more hopeful about how we navigate and get to the other side of this? Or are we not at the hopeful point yet?

**SINHA:** If we're looking for a time when this problem goes away, it'll never happen. But that doesn't mean that you lose hope. The basic cyber hygiene, basic cyber security strategy, has to be in place. We cannot live without it. But that doesn't mean that we should change our lifestyle. That doesn't mean that we should change who we are, how we interact, how we transact, how we work, how we collaborate. We just need to ensure that we are doing our part. Organizations are doing their part. And together we contain this.

I feel like, with or without this war, all of us have to pay attention to the fact that free and open societies will always have a soft underbelly. And, how do we ensure that we protect ourselves and protect our society and still be open?

**SAFIAN:** Yeah. Well thank you Bipul, this has been great. Thank you for joining us.

**SINHA:** Thank you so much for this opportunity Bob, and nice to talk to you.