PODCAST TOPIC: FUTURE OF CYBERSECURITY

You are listening to the OneHCL podcast series, the place where industry experts, analysts and veterans help us identify, understand and prepare for the upcoming cybersecurity technologies and trends. If you haven't subscribed to our channel already, do it now for regular updates. In this podcast, we have with us Kristina Elestedt-Jansson who will be sharing her views on how evolution of cybersecurity will impact us in the coming decade. This episode starts in 3 2 1 –

Now, could you please introduce yourself?

Yeah. Hi, my name is Kristen Elestedt-Jansson, and I'm head of CyberSecurity Fusion Center in Sweden. And I've been in the IT world since many years, and started up as an application developer, I worked with the infrastructure area. And for 20 years, I've been in the security field.

Q.1 Kristina, could you shed some light on how future companies will evolve in terms of their approach towards cybersecurity?

Yeah, security up till today, not been on top of the board's agenda, I think all of us working in the security field will recognize this. And with the changes in the cyber world today, and looking into the future, the world has changed, and will continue to change, which means that companies must focus security to survive, it will be a benefit during marketing activities, and it will attract new customers. Similar to how companies today are using environmental and corporate social responsibilities activity. It's all about image. And I do believe that companies developing security products will cooperate. And I think we will have more niche vendors who will, together with other companies, corporate between each other to secure that all areas are covered, and that the products can exist and work together. And companies delivering the goods and services must increase the security footprint to both companies and consumers. And companies don't share anything when they are on the security threats. But they will need to be better in doing this and they must be open and honest amongst companies to inform when they are under attack. Today, no one talks about this because companies believe that their brand will be destroyed. But moving forward, this will be a winning concept. Be open and honest, this is the only way to beat the criminals. And since we all are working from anywhere, and perimeter protection will not be necessary anymore, some perimeter protection will exist. But instead, the security will be based on the role you have information classification in place and device. And the companies will have a very advanced developed identity and access management system for control since there's access for you. So, depending on where you connect from, you will be able to access different parts of the application, and sometimes even need to go to the office if you're supposed to access very sensitive information.

And since we are humans, and employees, we will always be the weakest link. So, companies will have advanced awareness trainings, many companies have that already today. But there will be much more focus on training employees. And, also to have a more ad hoc way of doing this if any user group or user starts behaving in a strange way. And I think that the companies in the future need to identify if they have any potential risk groups behaving in a strange way during their daily work.

Q.2 That was very insightful. Christina, I'm sure our listeners would also want to know the other side of the story, which is how cybersecurity will play a vital role in shaping up the society of the future from a people perspective.

Yeah, yes, we are most important in all sense. I mean, people are already today, more or less connected 24x7 and there is a lot of information that is recorded about us and it is beneficial for us as users because it gives a better experience of a specific service, but it's also a large drawback as more information is gathered and this must be controlled and thought in a very specific way, and not to jeopardize the personal integrity, and we have a number of laws, GDPR coming up. And in most cases, the user needs to give some kind of consent to handle all the information. But if we should be able to protect people from the cyber criminals, I'm not sure that this will work in the future, to be able to utilize the cybersecurity products that are available already today and will be enhanced even more in the future, in the best way, we need to know even more about, and use compared to today. And this means that we need to record more information about the user to understand who's behind the device. Today, we already have a lot of security products in, for instance, our course, in the future, there will be another dimension involving the driver or even all the passengers in a car. And depending on what is happening inside the car and outside the car, the car will change the way of driving. So, preferences will be more and more automatically set based on people's way of behaving. And the question is how preferences can be changed in the future if the person changed their way of living? Will the preferences be based on last year or what will be the context? Devices will also be capable to monitor psychological signals and combine the information with environmental preferences it has already learned from the user to create the ideal environment. And I don't think we will need to type any passwords, (which we all have issues to remember) is that user biometrics will be used for different applications and systems and the cybersecurity products will support with efficient ways of utilizing both passive and active biometrics awareness trainings, as we have in companies already today. But the society needs to take a larger responsibility to build awareness amongst all the sectors and not only people working in the company to secure that we all know how to behave and understand the risk we can be exposed for when utilizing services in the current world. It has started already in schools, so our children will be well-prepared for the future.

Q.3 Yes, Christina, that is something to really think upon. On this note, would you like to share any closing points?

Yeah, the digital journey will increase heavily during the coming years. And this will also lead to a broader threat landscape. Unfortunately, it will be more and more difficult to protect individuals, companies and the society and we already see demands from different parts of the society that we need to change our view on. What cybercrime actually is, that the digital world needs a new perspective. Everything boils down to that we need to think in another way and be more global and open for new ways of working, at least within the cyber world. The society has always tried to protect their citizens. But when we move into the cyber world, it's not that easy. The borders don't exist anymore, and it's difficult to know whom to protect the citizen from unfortunately, we as humans will always be the weakest link and how do we reduce the risk of the humans to do wrong? How do the society support them in the digital connectivity?
I believe that the focus will be on protecting paper from cyber criminals rather than protecting the privacy.

This episode of the OneHCL podcast series has ended. Be sure to subscribe for more insights on how to identify, understand and prepare for the world of possibilities around the new and upcoming cybersecurity technologies and trends. Don’t forget to rate and review the episode so that we can keep bringing you the most relevant content. Thank you for listening!