You are listening to the One HCL Podcast series the place where industry experts, analysts and veterans helps us identify, understand and prepare for the upcoming cybersecurity technologies and trends. If you haven't subscribed for the channel already, do it now for regular updates.
This episode starts in 3-2-1

Hello There! What a ride year 2020 has been! Like you I am too reeling from the impact and still compiling the learning from the bygone year. There is so much that we learnt last year, didn't we? So we decided to make it a subject for this edition of our podcast. Before you say another one of the new normal or human resiliency or anything of that nature, here is a pledge, I am not going to talk about any such clichés.
My attention is going to be on sharing my observations about the data protection controls that were put to test last year and what we observed through the what is point of a security professional. How did we fair, on that the jury is still out but there is some learnings already. So why don't we talk about it, I am going to do just that in this edition. Ladies and gentlemen I am Amit Mishra your host for this edition, to start with a particular incident involving a tool that perfectly characterized last year and talking about the poster boy for the year 2020 the zoom video conferencing application. Zoom and similar conference application make sure that can be used to operate and collaborate essential tool kit for resilience and suddenly there when use of zoom meeting is getting compromised. Some embarrassing or sometimes hilarious incident some what we now know as room money started getting reported at this point we must Clarify that it was not any vulnerability in zoom that caused it happen through a method what we generally call credential stuffing. Just to break it down make it simple addition stuffing is all about exploiting careless attitude of users tend to use similar kind of credentials for all kind of applications. whether it is official or personal use regardless of these conditions are stored in which website they are using it in for it so all hacker has to do is just this kind of username password players from grey market and its and username password they try on all kind of applications that then lay their hands on just try their luck on and in this particular case it turns out that in zoom meetings many of these username password pair they hit the jackpot. So Bingo they found a way to get into your zoom meeting and invited and US rather than making remote working possible these tools are also became new avenues of cyber-attacks and the potential new that vector. So while everyone agrees that the third surface is increased when you still don't know what is the role of rise user played in such compromises by just being the necklace that it was not lost on the cyber security professionals. Year 2020 was different in multiple ways but when it comes to the cybersecurity and was no difference was again the think in armor and out to be occurring or reckless handling disgruntled employee and exactly the same order. As long as they are human beings need authorize access to data that is system will have to deal with your own weaknesses that can't be addressed by technology alone I know that this is not a relation to you my point is more to do with how this factor becomes even more pronounced in new way of working just to dwell little bit longer on that particular point so that I am sure that I've been able to convey my point across. Let me take you to another incident that happened last year in a large pharma major they went through not one but three breaches in one year in first it involved the former employee in second it involved current employees spouse and in third it was a contractor caused the breach. First case was out right

illegal usage of data because an ex-employee had no business in accepting that is system access that he had while he was still employed so his motive can be question and but in the process it also exposes the weaknesses in the IT security controls. In the second case it was one authorized employed allowed his spouse to use this official laptop in the spouse return the favor by downloading a file sharing application these applications are already notorious for carrying malware with it head and this particular application didn't disappoint. It brought in a malware and that cause the Mayhem. In the third case The contractor lost his laptop and along with it tons of sensitive data the contractor he didn't have a bad motive, it was an innocent mistake but still a reckless one. So when you look into these incidents in totality when you start feeling the layers in each of these incidents and look for commonality. You will realize that these incidents were caused by the IT security controls which placed too much faith in the security awareness of the authorized user and thereby providing the keys to kingdom. In Other words, the security controls were limited to controlling unauthorized users but when the system was accessed by other authorized users, it allowed them a free pass for their action. And no matter how unusual these actions were, it didn't trigger any alarms. That brings me to the subject of this podcast this is the moment of truth. Year 2020 tested our data protection controls limit and guess what we found. A realization that focus of current cybersecurity architecture focuses generally to prevent unauthorized access not on preventing unauthorized usage. This sentence sounds counter intuitive so I will repeat that. I am referring to the current cybersecurity architecture which generally configured to prevent unauthorized access but it does very little in unauthorized usage. What I am not saying explicitly is that this unauthorized usage could be from authorized user they are not the same thing and both are equally important. To put it differently while we are sinking in millions of dollars to build, defend against unauthorized access to our IT systems and data. I mean to say are we showing same urgency to build controls to spot unauthorized use of data by the authorized users. Aren't we placing too much trust in authorized users and their infallibility. Aren't we turning a blind eye when an authorized user is accessing our critical IT systems and data. If you are following where I am trying to lead you with this, the issue I am referring to is absence of any knowledge about our obligation about the data we have access to. Our capability to understand and define what is right and lawful usage of data. Our lack of knowledge about the business purpose of data that we have access to. Year 2020 amplified this weakness and no wonder a lot of IT enterprises have woken up for the need of having the control that is based on data and not the user. Once again another counter intuitive point, essentially what I am trying to refer to it, So far the control were tuned based on users and their roles in enterprise time has come to change that paradigm and start looking into the data that build the controls. That in my opinion is the biggest learning of the bygone year. This learning calls for some retrospection with the benefit of hindsight now we can easily say that here are 3 controls using them could have made our life much easier. Without any further delay lets go to that list. First on the list is the topic of data governance, to put it simply data governance

Is a means to try to develop understanding purpose and ownership of data. Idea is unless you know the purpose of the data there is no way you can determine if it being use for business purposes or not. Establish accountability of data usage, there is no shortcut to attain just that without having the well-Conceived data governance would have worked.

Second point talks about key point I have been harping about since the start of this podcast. That point deals with insider threat. So second In the list is capability to detect insider threat authorized users seems to have free passes to resources was there pass last old bridge. Many enterprises don't have controls that checks every so sensitive data even if you know they have this controls and not implying that such controls will make the system fullproof. But all I am merely trying to indicate that when you have controls which are looking into every access of sensitive data at least it can do is to provide you data point enough Data points for your threat detection solution to decide for and smell write when there is one. Third control or third learning deals with the accountability of the users in most cases the user should cause the breach were not even aware of the sensitivity of the data that they had access to. Funnily enough in many cases they didn't even know the level of access that in the system. Most enterprises have a generic program in building awareness about the privacy of data and program to make them aware of techniques used by cunning social engineers are fishing campaigns. These programs are at a very general level they just write a more general knowledge what I have referred to here is about having more specific knowledge about exact data that these users have access to and what all kind of application it brings a lock. So what like is a program to make them aware of their current level of access to suggest to go past that and this time taken with the argument of ignorance from the use of dat. How you do that by involving then the data governance program that I referred to as first in our list of learning. Data governance programs provide a framework for all the users of the data to collaborate and arrive at you know building up bigger picture about the data that they have in enterprise controls together can help enterprise increase accountability of data usage that may help in a pandemic kind of event with much ease. Assuming year 2020 was not one of aberration in our otherwise predictable life these learning surprised us and prepare us for a holistic approach to data protection thank you for listening to me hope you enjoyed this edition with that allow your host Amit Mishra to sign off.

This Episode of the One HCL Podcast series has ended, but 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.