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

The objective of this podcast is to talk about the challenges faced by organizations to determine the right IT security framework. There is a plethora of information out there pertaining to security programs and frameworks, and with all these different options to pick from, how do you choose? Let's hear our speaker. Hi Chandrashekhar, can you please introduce yourself?

Hello Devleen. First of all, thank you for having me. My name is Chandrasekhar Moharir, but most people know me by Shekhar and I'm currently working as a group manager in our GRC practice. From professional experience standpoint, I have close to 20 years of comprehensive experience in different areas of information security, such as consulting, compliance, audit, risk management, business continuity, and disaster recovery management in GRC platforms like RSA Archer. That being said, I was directly engaged in helping many enterprise across multiple industry verticals transform the GRC program from either non-existent or ad hoc in nature to fully controlled, quantified, and further optimized

Thanks for the introduction Shekhar. So diving in can you shed some light on What is an IT Security Framework and most common or industry specific frameworks leveraged today?

That's a good question, let me start with an it security framework and it security framework, in my opinion, can be considered as the building block of an enterprise's security program, which typically contains a number of documents, such as policies, procedures, and processes that will apply to an enterprise it security practice. And when such a framework implemented properly, it greatly helps an enterprise manage their overall security risk landscape. Now, having said that a framework should theoretically make planning and implementation of security easier, but in fact, the actual struggle starts when you want to select the right Preet security frameworks, especially when there are so many to choose from. Now from the popularity and the adoption standpoint, I think frameworks like NIST ISO two seven zero zero one COBIT and CIS top 20 are the most popular, or I must say most common frameworks that security professionals are aware of.
And lastly, I want to mention that there are security frameworks that are driven by industry specific compliance requirements like high-trust, which is specifically designed for healthcare sector. Next, I want to mention its cloud security. Alliance's cloud security matrix that is designed for cloud service providers and PC ideas, DSS, which is a set of requirements designed to ensure that all companies, that store process, or kind of transmit credit card information, maintain the secure environment.

Shekhar you made a great point about IT Security framework being the building block of an enterprise's security program. What should be the approach for an enterprise in choosing the Right Security Framework to Fit their Business?

This is again, a very interesting question, and one can spend an entire day talking about it. And that being said, I will emphasize on some of the key points that an enterprise should concentrate on during the selection of a right, security framework. Basically a structured approach for selecting an appropriate security framework starts with understanding the security and regulatory requirements, along with risks that are unique to your business and to your industry.

Speaking of regulatory or compliance requirements, many industries such as healthcare, government, and finance have to follow industry specific security compliance requirements that are set forth in HIPAA GLBA or FISMA. And these are, you know, again, well known security frameworks as well. The second aspect is to understand and keep in mind a security framework is meant to provide guidance, to manage security risk and should not be followed blindly. I want to emphasize on the word blindly, because, you know, with that said, I strongly feel that before getting into the weeds of understanding specific security frameworks like ISO or NIST, and there are specific requirements in an enterprise should always keep one thing in mind that they can always create and implement a hybrid security framework, which is nothing but cherry pick guidelines and security controls from the different security frameworks to address organization or business specific risk. And last but not the least security framework, should we choose them on the business needs and not on what is popular or training.

You know, the reason for me calling these out specifically is that predominantly we have also heard in the past that many enterprises focus on selecting and implementing the most popular security framework and kind of lose focus on actual requirements over to w shaker.

Shekhar, you spoke about the basics of IT Security Framework, types of frameworks & how to implement it. I am sure our listeners would like to know how are we at HCL are helping Enterprises select right security framework?

Sure. Let me start by mentioning that there are various ways that an enterprise can choose from while selecting appropriate security framework for themselves, but we at their scale passionately believe the journey to select and implement best fit security framework starts with understanding regulations that an enterprise is governed by and risk faced by an enterprise. Next important step, we kind of focus on is to understand business functions that are most critical and represent highest risk to an organization by leveraging risk based approach.

What does it help is to us prioritize the implementation scope of the selected security framework and then comes gap assessment of security documentation? This kind of takes me to the next logical step I want to talk about, which is to asses the effectiveness and efficiency of existing security policies,

procedures, and processes. Furthermore, this tape helps us understand alignment of existing security documentation to the regulatory requirement, if any, and also the popular security frameworks. This also gives us an opportunity to save time during the implementation phase, by building upon or using this existing security documentation, if appropriate. And finally, yet importantly, I would like to talk about that, we focus on making top management aware about the importance of using security framework and benefits offered because of its implementation.

That was very insightful! Can you also shed some light on How HCL is helping Enterprises in implementing the right security framework?

This is an excellent question. Since one can easily lose focus on the implementation piece of security framework while discussing obstacle framework. Well, here it goes, goes without saying, instead of beating around the Bush, we start the process by developing system security plan, which, you know, many people will call it as SSP, which provides an overview of the security requirements of the system and describe the security controls that are in place or plan to be implemented in order to meet the risk identified remove to make this plan grow. We take regulatory and the compliance requirement into consideration throughout its development. Now tailoring the security framework to your business needs is easier said than done and cannot be achieved without understanding the current security of the enterprise. How we accomplish this goal is by email evaluating current security posture and identification of security gaps by performing maturity assessment followed by documenting plan of action and milestones for each gap identified during maturity assessment as a final point and what I emphasize in order to address complexity phase by an enterprise during the implementation of tailored security framework, we at HCL created a proprietary framework called brakes, which hosting in concentrate on is the alignment of business and ID compliance requirements.

The next area we focus on is we kind of blend process and operational methodologies from most common and popular security frameworks, like COBIT ISO NIST, CIS to help implementation of hybrid system. And lastly it leverage SCLC [inaudible] control framework for selection of tailored security control. And since I mentioned UCF, let me speak briefly about it. UCF here is a library of global regulations and 25,000 plus security controls along with their definitions for easy access.

do you like to share any final thoughts on the road ahead? Sure. Let me start by saying there is, there's no such thing as one size fits all approach to security and each framework own pros and cons. Having said that organizations vary in complexity and maturity from the security standpoint, for the same reason, it is extremely important to research the available security frameworks and balance the benefits and drawbacks of each approach.

Next thing I want to mention is instead of adopting single security framework from soup to nuts, a hybrid security framework can be proved helpful for an enterprise to meet their unique business objectives and compliance requirement. Another topic that one should focus on is to understand security gap, which in my opinion, will play a major role in addressing regulatory obligation and protecting an organization from security breach. And finally, I want to conclude the talk by mentioning whichever framework or the combination of framework and enterprise selects, a comprehensive

strategy to defend against potential threats while keeping data secure is more crucial than ever. Thank you over to you, devleen

Thank you, Shekhar for your insights and thank you for being part of this podcast. I'm sure our listeners had a lot to take away from this discussion.

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.