Shilpa Sawant

Assistant Vice President Cyber Security, Reliance Industries Limited

Briefs about cyber security and risk management as well as data privacy

Interview of Shilpa Sawant, Assistant Vice President, Cyber Security, Reliance Industries Limited.

Do briefly tell us about your journey so far.

I am a Cyber Security Professional with 14 years of experience and presently working as an Assistant Vice President with Reliance Industries. An Education background of B Tech in IT and a Masters in Networking chalked my path into this field.

The journey so far has been overwhelming and equally challenging. As the Cyber Security field has been evolving and advancing, there is always an innovation involved to keep up or be ahead in the race. I believe that the best part of being in Cyber Security is that it's a dual role that we need to play - the battle is always with the external world and the internal world. While we are always in a state of defending against cyber-attacks in the external world, there is also a need to justify or make businesses and users understand the importance of Cyber Security, which is equally, if not more, challenging. While there are tools and technologies to protect against external attacks, it was essential to develop strong interpersonal skills, the right attitude, as well as exclusive strategies to handle the stakeholders and enable the business securely. In addition to this, the learning

Shilpa Sawant
Assistant Vice President - Cyber Security,
Reliance Industries Limited

> **The success of the Cyber Security Program depends on having a sound security strategy encompassing preventive and detective measures, simplified processes, awareness, and intelligence-driven security operations along with a plan of continuous improvement.**

curve never ends in this field. It is imperative to be aware of the trends and advancements in technologies and adversarial tactics.

Recognition and acknowledgment within this fraternity as well as certifications such as CISM and CISA from ISACA have added as a motivation factor to achieve and contribute more.

This decade-long experience with India's biggest conglomerate gave me to an opportunity to work at a group level on different domains, complex environments with diverse and large businesses having unique compliance requirements.

My expertise has been mainly around cyber security strategy, IT and security risk management, devising innovative approaches, frameworks and solutions, governance, vulnerability management programs, cyber security architecture, awareness, compliance, and the latest being Security in digital transformation. This broad exposure has been quite fulfilling, and I still consider myself to be in the 1st mile of my journey. There is still much more to contribute to the community to make this digital world a secure space to live in.

Briefly share your contribution in improving an organisation's efficiency & data security.

The success of the Cyber Security Program depends on having a sound security strategy encompassing preventive and detective measures, simplified processes, awareness, intelligence-driven security operations along with a plan of continuous improvement. I was involved in completely transforming the organization from erstwhile Information Security to Information Risk Management. This necessitated in setting up comprehensive policies of the group, appropriate technology controls, and embedding a Cyber Security Culture with continuous awareness within the businesses. Continual improvement initiatives were initiated to improve the maturity level and benchmark against the best practices. Developing and implementing innovative security frameworks such as competency frameworks, new-age IT technologies have been my forte.

Executing a Cyber Security Awareness Program where I had to periodically launch out-of-the-box campaigns making the organization realize the importance of Cyber hygiene, and encouraging users to practice Cyber Appropriate Behavior. This has been

personally satisfying, as now we have enabled & empowered more people to be part of the Cyber arsenal.

A good governance structure is critical for measuring the performance of any function. Overseeing the cyber security programs and operations for all the group companies regularly and identifying improvement areas has immensely helped the organization improve its efficiency.

In spite of the latest technology and software being used why are the cyber-attacks increasing? How can it be secured?

According to me, this is the only field that has been so dynamic. Outlook of the Cyber Security practitioner and strategy changes almost every 2 years. Earlier, it was prevention, then CISOs focused on prevention plus detection, proactive detection and now, as cyber-attacks are inevitable, the strategy is around cyber resiliency.

While organizations are revolutionizing their digital landscape and adopting next-generation technologies to launch digital platforms, this unfolds new attack avenues and provides a platform for cybercriminals to penetrate into the network.

Cyber-attacks have become more sophisticated, where the adversaries today are using advanced technologies such as AI/ML & innovative techniques to launch attacks. The motive of attackers has transformed over the years. The target of cybercriminals is not an organization anymore but industry or the state or the nation. In the Darkweb, the underground economy, launching attacks on an organization is offered as a service.

With this kind of evolving landscape, Cyber Security Solution providers and product companies are forced to think at least 2 steps ahead before they launch a new product or feature, or functionality. It has also brought industries together where this is collaboration and strategies defined for a common goal.

It's a huge challenge for the cyber security teams to justify the investments as the threats are growing manifold and existing solutions may not be effective to detect all the new

variants. Hence, practitioners are also focussing on developing homegrown approaches and solutions to address the risk. This brings another challenge of skilled resources to develop and maintain the solutions. As cyber threats show no signs of slowing down and with cyber talent drought, organizations are still at high risk, despite investing so much in defense technologies.

There is no silver bullet to achieve the desired state - efforts have to be put in the areas of people, process, and technology. A risk-based approach should be embraced to fortify defenses and seamlessly integrated Security into business processes to protect critical data.

Share one of the most interesting assignments that you handled.

While gaining knowledge on the technical aspects of Cyber Security keeps me on my toes, executing Cyber Security Awareness Campaigns is something that I'm passionate about. It is like pursuing a target that is always moving and that in itself is taken up as a challenge to go after and beat time over time.

Phishing Attacks are one of the growing concerns for any organization today. Although numerous approaches have been developed to detect and prevent phishing attacks yet there is no foolproof solution that can detect and prevent 100% of phishing attacks. The tactics tried by cybercriminals are very sophisticated where they try to exploit the cognitive thinking of users. Therefore, Humans here become the 1st line of defense, not the last line of defense as most cybercriminals try to obtain initial access or foothold into the network using phishing tactics. Strengthening the human firewall needs a detailed study on behavioral design and psychology. The program that I was instrumental in developing has proven to be a game-changer in our domain. It is based on an iterative E-E-E lifecycle – Educate, Evaluate and Elevate and strives to make users resistant to phishing. This led me to the research mode on Cyber psychology and the behavior patterns of users and then based on that formulate a program on varying human behavior to ensure users don't fall prey to phishing attacks irrespective of their emotional state. This being an iterative program, knowing the user's susceptibility factor and accordingly planning the next action is quite revolutionary in today's times. This programs' success has not only helped users identify any form of phishing attacks but is recognized to be a strong cyber defense control – the first one of its kind. A&S