# The Cybersecurity Readiness Podcast

**With Dr. Dave Chatterjee**


## Going Above and Beyond the Mandated Checklist

**Guest** – Tushar Sachdev, Executive Vice President and Chief Technology Officer, KORE Wireless

### Summary

When top management proactively takes every possible precaution to protect sensitive data because it is the right thing to do and not because there is a legislative requirement, that's when the organization would have taken a huge step forward in earning customer confidence and trust. Tushar Sachdev, Executive Vice President and Chief Technology Officer, KORE Wireles, is emphatic about top management's role in creating and sustaining a proactive information security culture. In a very reflective and pragmatic discussion with Dr. Chatterjee, Mr. Sachdev, also offers guidance on how to a) get started on a path to cybersecurity readiness; b) reach a high state of cybersecurity readiness; c) get senior executive commitment to cybersecurity training; and d) select and monitor suppliers. He also talks about the importance of including cybersecurity performance metrics in performance appraisals and buying cyber insurance.

# Key Takeaways

**(Prepared by Dr. Dave Chatterjee)**

## Memorable Tushar Sachdev Statements and Quotes

- Security is an organization-wide responsibility -- it includes marketing, customer support, HR, operations, it includes the CEO, and it includes the Board of Directors.
- Just like you practice meditation, you should practice information security with the same dedication and discipline.

## Role of Top Management in Creating and Sustaining a Proactive Information Security Culture

Top management can play an important role in:

- Bringing about a culture change, whereby there is organization-wide recognition that information security is everyone's responsibility.
- Encouraging and supporting continuous cybersecurity education across all functions and roles. From Marketing to Customer Support, HR, CEO, and Board of Directors, there needs to be a greater level of knowledge and awareness of how and why security breaches happen, the consequences of such attacks, and how best to prevent such attacks.
- Ensuring that cybersecurity preparedness is a regular discussion item at Executive Leadership meetings and Board of Director meetings.

## How Do You Get Started on a Path to Cybersecurity Readiness?

- First, getting to know all the data and systems of the company. Getting to know where all the data resides and where all the systems (that are processing, storing, and disseminating information) are located. This is not an easy task given the complexity of organizational information networks and data flows and the existence and proliferation of shadow IT environments within the organization.

- Second, identifying where the organizational vulnerabilities and risks lie. Mapping vulnerabilities to risks is key and doing a Cyber Risk-Impact Analyses should be a starting point for creating a comprehensive cybersecurity governance plan.

- Protecting customer data should be the priority because breach of such data has the most adverse consequences ranging from all kinds of liability issues to lawsuits.
- Be selective when selecting external consultant. Use only those who have an in-depth understanding of your organization and industry. Do not buy into a cookie-cutter solution.
- If the organization is operating within a very niche domain, every effort should be made to develop in-house cybersecurity awareness and capabilities.

## Getting To A High State of Cybersecurity Readiness -- Success Factors and Challenges

### *Success Factors*

- **Commitment** at all functional levels such as: information security, information technology, software development, marketing, operations, HR, legal, and operations. Very supportive and proactive senior leadership team and board of directors.
- **Education** – Developing an in-depth understanding of security issues – from vulnerabilities, types of attacks, defense mechanisms, and more.
- **Prioritization** – Prioritize your information security budget and spend.
- **Discipline -** Sound information security practices are etched into the organizational DNA and institutionalized.
- **Staying a Step Ahead** – Through continuous learning, investment, and adoption of other security best practices, the organization stays abreast of the latest cyber-attacks and threats.

### *Challenges*

- **Siloed Mindse**t – Statements such as "I need to focus on my functional goals and objectives. Security is not my concern or responsibility," is a reflection of a siloed mindset that is not conducive to effective cybersecurity governance.
- **Human Factor --** Lack of focus on people related information security vulnerabilities

## Getting Senior Executive Commitment to Cybersecurity training

- **Explain – Incentivize – Punish**

  Tell them what other organizations are doing and the consequences of not staying current on cybersecurity matters. Incentivize senior leadership commitment to continuous cyber training. Punitive measures should be used as a last resort to achieve compliance.

## Supplier Selection and Monitoring

- The first step is to know your suppliers. Identify all suppliers and map them to the contracted tasks and activities.
- Make sure you are treating suppliers as employees. Give them the same level of cybersecurity training as your employees.
- Have the same security standards and expectation for your suppliers and contractors as you have for your own employees.
- Getting the supplier to check all the boxes of a security questionnaire is not enough. That is just a starting point. Make sure the supplier organization is genuinely strong in security, provide close oversight, continuously monitor the organization, and look out for ownership changes.
- When interacting with suppliers, data should be shared in a very secure manner.
- Buying joint insurance or some other way of increasing supplier liability is a challenge that industry needs to crack. Tying a small but good supplier to a larger liability could result in losing that supplier.

## Cybersecurity as Part of Performance Appraisal

- Having cybersecurity as part of employee performance appraisal is worthy of consideration.
- Organizations get scored on security when it comes to responding to an RFP or a tender evaluation scorecard.

## Cybersecurity Insurance

- Cybersecurity insurance is a must to deal with post-breach labilities and other consequences. The insurance amount needs to be determined by hiring actuarial and other experts.