The Cybersecurity Readiness Podcast

With Dr. Dave Chatterjee

Role of Top Management in Cybersecurity Governance

Guest -- Rohit Verma, CEO, Crawford and Company

Summary

The recent ransomware attacks on Colonial Pipeline and JBS are grave reminders that organizations at all levels must constantly be at a high state of cybersecurity readiness and alert. This is no easy task as the points of vulnerabilities are numerous, especially the probability of humans falling prey to innovative hacking maneuvers. The senior leadership has an incredibly important and critical role to play in securing operations, sensitive data, and other digital assets. They must actively engage in the planning and execution of cybersecurity governance activities and spearhead the creation and sustenance of a high-performance information security culture. Such a high-performance information security culture is anchored on three key pillars – commitment, preparedness, and discipline. **Dr. Dave Chatterjee's book on** Cybersecurity Readiness: A Holistic and High-Performance Approach speaks to these security culture traits and associated success factors. Probably the most important success factor is a highly committed and engaged top management. In an extensive and insightful discussion with Dr. Chatterjee, **Rohit Verma, CEO of Crawford and Company**, speaks candidly on topics ranging from top management involvement to empowerment of the Chief Information Security Officer (CISO), cyber training and assessment, intelligence monitoring, performance tracking and measurement, security drills, and best practices.

Key Takeaways

(Prepared by Dr. Dave Chatterjee)

Memorable Rohit Verma Statements and Quotes

1. Approach cybersecurity at work with the same genuineness and care as you would when securing your own home and family.
2. If leadership of other organizations need any convincing about staying up with cyber training, all they need to do is look up the WSJ for the last three months and read about the extent of havoc cybersecurity can cause an organization. Cost of recovering from the attack is quite significant. Clearly, "prevention is better than cure."
3. Several of us in senior leadership are digital immigrants and not digital natives. Many of the security issues are new to us. We will be naïve if we don't take interest and are not willing to learn and stay updated.
4. Growth mindset and empowerment are two key drivers of the organization's approach to cybersecurity preparedness. Instilling the 'Growth Mindset' in organizational members implies three things – everyone has something to learn; capabilities can be expanded; keep an open mind.

Top Management Involvement

1. Senior leadership takes cybersecurity very seriously and is totally committed to taking all necessary measures and steps to protect sensitive data and related assets.
2. Cybersecurity readiness is a strategic imperative for Crawford and Company. It is imperative at the Board level; it is an imperative at the Executive level.
3. The CEO also takes ownership and responsibility to protect and secure organizational data and related assets.
4. State of cyber readiness is a regular agenda item at company Board meetings where the CISO presents to the Audit Committee. There is an ongoing dialogue on how to continuously secure the organization from evolving attack types.

CISO Empowerment

1. The Chief Information Security Officer (CISO) who reports directly to the President, is fully empowered to take any necessary steps to fully secure the organization.
2. The CISO is also supported with a strong team.

Cyber Training and Assessment

1. Cyber training is mandatory. Cyber training programs are customized to fit the different organizational roles and responsibilities.
2. Assessment mechanisms such as mock phishing attacks are used to gauge cyber training effectiveness. They also have targeted sessions with groups that did not perform well during the tests.
3. Level of cyber awareness and alertness is regularly tracked.

Intelligence Monitoring and Documentation

1. There is constant monitoring of threats.
2. Chief Privacy Officer and Chief Information Security Officer work hand-in-hand and also with external partners to monitor the environment, gather intelligence, and act promptly. Rohit believes in having a clear trail of records documenting intelligence gathering and processing.
3. The organization leverages the information security expertise of business partners to stay abreast of the latest types of threats and defense mechanisms.

Performance Tracking and Measurement

1. They have developed a framework to assess cyber readiness across various dimensions. CISO working with the CIO is responsible for driving that framework in partnership with the business-unit presidents and CEO.
2. They monitor a portfolio of metrices.

Security Drills

1. A company best practice is the seriousness and diligence with which they conduct their annual tabletop exercise to simulate cyber-attacks and assess the organization's ability to recover from the attack quickly and effectively.

Best Practices

1. The extent and level of visibility the CISO enjoys in the organization
2. The extreme seriousness and diligence with which the organization carries out the tabletop exercises.