The Millenium Alliance – Executive Roundtable

October 22nd at Noon

"Finding the Balance: Creating a Healthy Relationship Between Security Needs and Business Success"

Moderated by:

Dave Chatterjee, Ph.D.

Visiting Professor, Pratt School of Engineering, Duke University

Author: Cybersecurity Readiness: The Holistic and High-Performance Approach
Host, The Cybersecurity Readiness Podcast
https://www.dchatte.com
https://www.linkedin.com/in/dchatte/

Agenda and Discussion Plan

1. **Introduction (5-10 min)**
2. **Security Goals vs Business Goals (15 min)**
    - Do you experience a conflict between security goals and business goals? How do you deal with it?
3. **Cybersecurity as a Strategic Opportunity (15 min)**
    - Is the senior leadership in your organization willing to consider cybersecurity as a strategic opportunity?
    - Is security treated as a strategic enabler in your organization?
4. **Strategic Alignment (15 min)**
    - How do you achieve and sustain alignment between overall business goals and information security objectives?
5. **Concluding Thoughts (5-10 min)**

Recommendations and Best Practices

Source: HTTPs://www. cybersecurityreadinesspodcast.com

These are excerpts from Dr. Dave Chatterjee's conversations with CEOs, CISOs, and other subject matter experts.

Security Goals vs Business Goals

1. "We are not in the business of saying No. I am not the gatekeeper for the organization and the business. I don't have the authority to tell the business not to do something. I can advise them on the risk, they can ask for my opinion, at the end of the day, the business has to decide what is best for them."
2. "We must understand and respect the organizational mission and culture."
3. "I am paid to be paranoid."
4. "You have to engage with the business and make sure they understand the cyber risks associated with their activities and processes."
5. "First and foremost, the most fundamental thing you've got to know as the CISO is the business of the organization that you're in. Because if you don't understand how the business operates, what it does, how it earns money, how it spends money, where it really makes its profit that funds other areas that have losses, then it's very hard for you to understand how to prioritize what security controls need to be put in place, and also how restrictive you can be without cutting off the lifeblood of the organization."
6. "We have created customized information security checklists and shared them with the different departments. The checklists are not a list of Dos and Don'ts. It is not about saying what you can't do. It is about guiding them on how they could accomplish their work-related goals without increasing the organization's risk exposure. Essentially, it is about helping organizational members make informed decisions."

7. "So a patient can recover from a data breach, but they might not be able to fully recover from lack of care. So that's where I really want to emphasize that cybersecurity is patient safety. And we all have to take it seriously, regardless of where we are in that healthcare ecosystem."

Cybersecurity as a Strategic Opportunity

8. “Cybersecurity readiness is a strategic imperative for my company. It is imperative at the Board level; it is an imperative at the Executive level. 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.”
9. “It all starts at the top. The C-Suite must make cybersecurity an integral part of organizational strategic plans and priorities. Leadership commitment is a must, and it all starts from there.”
10. "Finding that balance of how the security function can be an enabler and a good partner within the organization."

Strategic Alignment

11. Security is an organization-wide responsibility -- it includes marketing, customer support, HR, operations, it includes the CEO, and it includes the Board of Directors.
12. “We have created an Infosec Champion’s network.” The Champions promote good information security practice within their business unit and share information security materials.”
13. The CEO also takes ownership and responsibility to protect and secure organizational data and related assets.