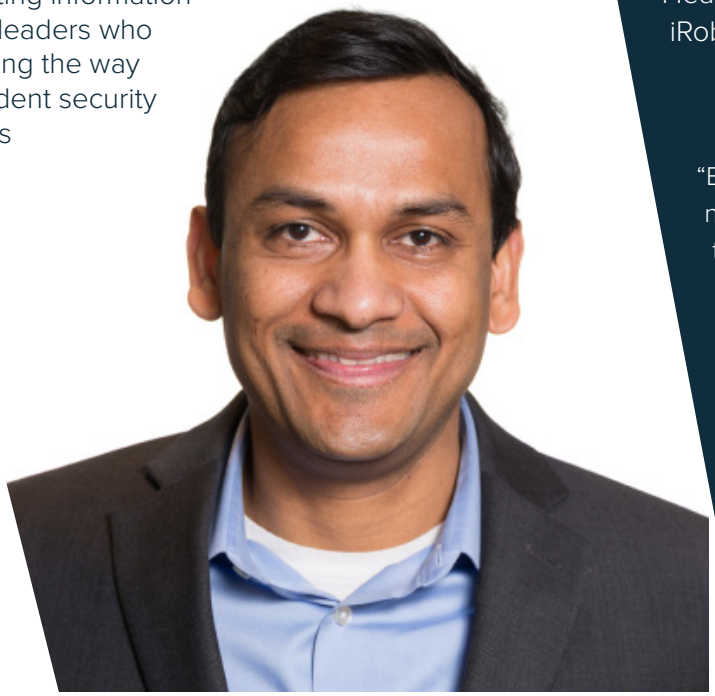
PROFILES IN CONFIDENCE

Highlighting information security leaders who are leading the way for confident security programs



RAVI THATAVARTHY

Head of Security
iRobot

"Being new to iRobot, the most important thing I need to do is establish indirect influence. I will do this by establishing key relationships with business executives, making an effort to get to know the people of iRobot, and understanding the culture. When they consult with me on a major project, or invite me to a project kick off, I know I have established indirect influence."

FOUR FACTORS TO SUCCESSFUL SECURITY PRACTICE

Previously the Head of Security at Haemonetics, Ravi Thatavarthy now heads the security team at iRobot Corporation, a leader in robotic technology-based solutions. When we spoke, Ravi had been at the helm of security for iRobot for only nine months, and still in the ramp-up and implementation phase of enhancing the company's security program. However, with years of experience and strong beliefs in his approach, Ravi has his game plan in place. At iRobot and other organizations he has worked at, he will follow these four key principles:

Communication with the Board

The board at iRobot understands the business value of security, and considers it a strategic imperative, which makes communicating with them fairly easy. Ravi strives to use the same context every time he speaks to the board, and to provide examples and comparisons from similar businesses. He says, "To be successful with the board, always present a plan and an answer."

Be in the People Business

Ravi's team strives to ensure that security is timely and provides "user delight". "User delight" means to avoid being a road-block or a drag on employee morale. To be in the people business you must understand the business goals of each department, from R&D to marketing,

sales, and beyond. Security teams may get bogged down in defending the company against threats, and as a result start to wrongly view employees as the bad guys. You must assume good intent. The R&D team just wants to do their job to the best of their ability.

Be Part of the Solution, Not Part of the Problem

"We are here to ensure security, not to stop business productivity," says Ravi. We need to present business leaders with the risks, but let them make the final decisions in terms of the risk they are comfortable with. "If you project risk in the right spirit, in your role as an indirect influencer, you have done your job successfully."

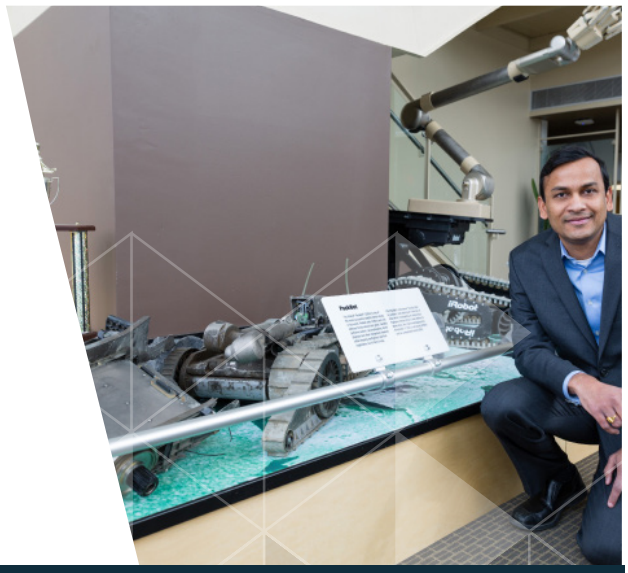
No Organization has Unlimited Budget for Security

Optimize the use of your existing security budget and leverage other efforts on top of that. Some security priorities have insufficient business value, so be creative to find funding for those efforts. Whenever possible, prioritize security with respect to business value.

"Be speedy, be flexible and be direct!" Ravi's approach to security comes down to business enablement. By networking with business leaders at iRobot and fostering a reputation for being accommodating, efficient and yes, likeable, Ravi reports that he is brought into more projects, which ensures security's place in the process.

"Some companies have huge security budgets and still get breached. For mid-size companies, the approach to security has to be about security awareness. Our employees have to be security aware, or else our program will not succeed."

- RAVI THATAVARTHY



A BUSINESS-FRIENDLY APPROACH

"I was delivering a speech about my business-enabling approach to security, and specifically talking about social networks and other sites that may open the company up to vulnerabilities. You cannot block access to these sites without losing the trust, ear, and collaboration of the employees. Some people certainly disagreed with me about this at the conference! In fact, there was a lot of opposition in the audience, and some walked out in the middle of my presentation. A few CISOs argued that you could never get a stronger security posture when allowing these sites on the network. I disagree. Security cannot be accomplished by only technical controls! If it is, emplodyees will simply work to circumvent the rules; and then you are less secure than ever. Use technology on the defensive, but do not use it on your own employees."