

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS
WHO ARE LEADING THE WAY
FOR CONFIDENT SECURITY
PROGRAMS



JP SAINI CTO, TRC COMPANIES, INC.

HEADQUARTERS: Windsor, CT

EMPLOYEES: 3,800

ANNUAL REVENUE: \$646 million

JP Saini has held the position of CTO and Head of Information Security at TRC for past 8 years, a national engineering, environmental consulting and construction management firm. In that 8 years he has evolved the Information Security program with commitment from the CEO and the CRO, and with a lot of hard work and effort put into the people-side of security. In fact, Saini says that his biggest challenge in business has been change management. “People tend to dilute the challenge of change management. It takes effort to effectively engage your target audience – employees, partners, clients, or the Board – to embrace changes in behavior.” While Saini lists change management as his biggest challenge, he has found success in the process.

“You have to invest in the people and prove the value of Information Security”

Success came because Saini put a premium on the human elements of Information Security. He says that it is important to put a few layers of security, including technology and processes around critical assets, but the most important step is securing the human element. “Many of the security organizations spend a lot of money on technology and process, they forget about the people,” says Saini. He believes this is a mistake. “You have to invest in the people and prove the value of Information Security.” This will engender change and make the organization more willing to embrace it. Saini says CISO’s must, “Find a way to continually present the outcomes of security efforts so that the credibility of the program is not lost.”

Showing results includes tracking annual and quarterly progress via reports for the Board, but is better explained to the company as a whole with anecdotes and progress updates. Saini says, “At the employee level we continually highlight any progress and updates that we can in the employee newsletter. Now, we cannot disclose every single detail to our employees because of employee turnover and confidentiality, but we are constantly communicating

at a high-level about the progress being made. We talk about ease-of-use, things to be aware of, and recent successes. The mind does not know what the eye does not see, so we put as much information as we can in front of people.”

Saini notes TRC’s employees’ willing adoption of self-implemented mobile device management as an example of effective change management that improved security. “We allow up to five devices – whether they are TRC provided or not. We put the instructions for enrolling on intranet, and people use it. If you make information meaningful, accessible and visible, your audience will respond to it.”

As Saini considers change management one of his biggest challenges, it is notable that he considers empowering TRC’s people as his greatest success. Saini says, “Beautiful things happen when you empower people, including your team, your peers, and your board. Empowerment does not mean that they have access to the cruise missile push button, but empowerment does give them access to information, and the authority to make smart decisions. Within the IT department at TRC we have empowered our people to be confident employees and we have seen great results, including high retention rates. People raise their hands to lead new projects and initiatives.”

WORKING WITH LEADERSHIP TO IDENTIFY SECURITY CONCERNS

Saini reports into the CFO who is also the Chief Risk Officer. He also works regularly with the company’s Senior Management team and Practice Leaders to ensure a security-focus in all projects that impact customers, partners, and employees. Saini reports both the CFO and the CEO are proponents of Information Security. The CEO is very interested in engaging in security discussions. Recently, TRC started a program to evaluate the Information Security strength of TRC’s many subcontractors. Leadership came together and decided that as the company strengthens its’ own security posture, it must also look at the posture of its’ subcontractor eco-system, because anything those companies do as agents of TRC impacts the organization. Saini has a leadership role in helping to evaluate and ensure subcontractor performance as it relates to security.

A FUTURE-FOCUSED APPROACH TO SECURITY

TRC is a company focused on growth and expansion. As a result, Saini spends a lot of his time evaluating and reporting on risks related to acquisitions and effectively combining and acquiring organizations into the company in a secure manner. The company is pursuing an ISO 27001 certification, which will ensure it meets international security standards. “ISO 27001 will allow us to effectively scale as we grow beyond the United States. We will not have to worry about changing our security practices to meet international standards,” said Saini.

BUSINESS ACUMEN ENSURES MORE EFFECTIVE SECURITY

Saini believes business expertise and acumen are becoming critical to effectively run Information Security programs. Saini believes business skills can be learned outside of the classroom as well. Saini says, “Business experience is a relative term. I do not think a business school will give you all those skills. You need to have the right level of business experience. You need to have a good mentor. Plus you need to have some formal training in understanding the basics of business. You can become a CISO because you are a great techy; to be a great leader you have to harness a few skills from the business side.”

The important thing is that CISOs understand how business functions so they can align security to business priorities. Saini says, “In my view, if you cannot run your own business, you cannot help anyone else run theirs. You have to be able to run any segment of an organization as a business. With a purely technical skill set it can be easy to get stuck in your own world and become too focused on the best technology or best certifications. You have to go beyond technology, process, and people and take a business approach. You have to understand what is happening in the market. What is driving the clients? This is your biggest strategic driver. Within the company you have to be able to sell security to the other stakeholders. That is easier to do when you understand their priorities.”