PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

NICK NEDOSTUP
CISO, JOHNSON CONTROLS

HEADQUARTERS: Cork, Ireland

EMPLOYEES: 120,000

ANNUAL REVENUE: $37.7 Billion

"We are constantly maturing our program, and doing everything possible to create a secure environment in ways that do not prohibit the business from meeting customer expectations and achieving our goals."

- NICK NEDOSTUP

THE CONVERGENCE OF PHYSICAL AND DIGITAL IDENTITIES

"There is a lot of focus in the information security industry on digital identities," explains Nick Nedostup, CISO at Johnson Controls. "But we also must consider physical identities, such as when someone enters a building, and which system controls - like lights or heating systems - they access. In the future, we must combine physical identity with digital footprints to track a person's complete identity as it relates to the enterprise."

When it comes to the convergence of physical and digital identity, few people have more direct experience than Nedostup. As CISO of Johnson Controls, which creates intelligent buildings, efficient energy solutions, integrated infrastructure and next generation transportation systems that work seamlessly together to deliver on the promise of smart cities and communities, Nedostup is responsible for the organization's enterprise cyber security program and is a major contributor and advisor to the company's Building Technologies & Solutions business development team.

One area of focus at Johnson Controls is the ability to help its customers' organizations understand and track physical and digital identity as one. "Our Buildings business development team is looking into the convergence of physical and cyber worlds, and exploring opportunities in the space," comments Nedostup. He works in a consulting capacity with the business, helping shape understanding around the capabilities of specific start-ups and to evaluate market demand as Johnson Controls considers new lines

of business, or adding security components to existing technologies.

Nedostup is a contributor to the company's business priorities in other ways as well. Johnson Controls sells many environmental controls which are now network-connected. He explains, "There was a big push to IoT, and early on I realized that security needed to be a component of these solutions. I raised this as a risk to the executive management team, and now I collaborate with the right leaders to build cyber security into our IoT 'Smart Building' products where appropriate."

He also plays a role as security advisor to the engineering team, and a sounding board for product development and marketing. "In the past, the client's CIO or CISO was not involved in purchase decisions. But now with these systems connecting to the network, information security has a seat at that table. I provide advice to our Buildings engineering team on what types of security controls should be built into the systems, and the specific concerns our clients' CISOs will have with the products," says Nedostup.

> "Being seen as a credible source is one of the most effective ways to grow the security budget."

ENABLE THE BUSINESS TO MEET CUSTOMER EXPECTATIONS

Nedostup's multifaceted role enables him to contribute to the solutions that impact the bottom line, while simultaneously maintaining the enterprise security program. Acquiring an MBA provided Nedostup a well-rounded, business-minded perspective. He says, "I understood that to provide real value to my organization and my internal customers, I needed to step outside of a traditional technology role, and shift into a business role. This shift allows me to see that security will never be the sole focus for an organization – we operate in the buildings and energy storage platforms. The function of information security, and I as the CISO, must enable the business to go forward in as secure a manner as possible, knowing we are not going to mitigate every risk. We are constantly maturing our program, and doing everything possible to create a secure environment in ways that do not prohibit the business from meeting customer expectations and achieving our goals."

Nedostup is proud of the achievements his team has made in the area of cyber security. "Our cybersecurity capabilities and maturity levels are far higher today than even a couple years ago. We've experienced rapid, focused and efficient advancement. We now have greater visibility into cyber issues, faster response times, and ability to contain and remediate threats." While these factors are critical to a strong security program, Nedostup says, "It's also critical that I serve as a trusted advisor to the business, that I have the ears and attention of our executives in understanding security as a risk area. We will always be refining what we do, of course, but I am proud that the security team operates at the business level, not just in the technology space."

BUILD CREDIBILITY TO GROW THE SECURITY BUDGET

Nedostup believes in the importance of building credibility with senior executives as a key element to grow the security program. He comments, "At times, I feel our industry focuses too heavily on fear, uncertainty, and doubt to drive program growth. But to be a trusted advisor to the other executives, I need to make them aware of risks, without blowing things out of proportion. Being seen as a credible source is one of the most effective ways to grow the security budget."

"Specifically, it is important to gain trust from the CIO, CFO and CEO – without it, it is rather difficult to be successful," suggests Nedostup. "That trust is built on being excellent stewards of our cybersecurity investment dollars, and ensuring we're supporting the business in every way necessary. We have to be purposeful and prudent in our requests, and be clear about how security investments enable the business to reach goals and mitigate risks."

Nedostup's effective campaign to build credibility and influence has enabled him to structure his team in a way that naturally and effectively aligns with the business. "Our team consists of experts from across the cybersecurity space, who are also knowledgeable about our business demands. We strive for continued partnership and alliance with the business to best enhance our cyber security program and effectiveness, and help the business achieve its growth and customer satisfaction goals."