PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

BRIAN NESGODA

CIO & SVP ENTERPRISE RISK MGMT
SIKORSKY FINANCIAL CREDIT UNION

HEADQUARTERS: Stratford, CT

EMPLOYEES: 135

ANNUAL REVENUE: $750 Million in Assets

Many CISOs believe the future of information security is as an autonomous unit outside of the IT organization, yet the majority of CISOs report into the CIO. At Sikorsky Financial Credit Union, Brian Nesgoda is pioneering a new path. Formerly the CISO, Nesgoda is now CIO and Senior Vice President of Enterprise Risk Management which includes the CISO responsibility. As he puts it, "IT now reports into security."

"The biggest challenge facing our industry is getting CISOs the visibility that they need within their organization. That means getting them out from behind the CIO and giving CISOs independence," explains Nesgoda. "Unfortunately, until auditors write recommendations addressing this conflict, we will see few changes industry-wide."

At Sikorsky, the organization is set up around risk. "We have a different structure than what you see out there [in other organizations] since IT reports into me. I hope to see more organizations make this change because I think it is long overdue for security to be at the top of the hill," says Nesgoda.

He continues, "As part of ISACA's CISO Working Forum, I speak with 30 other CISOs and hear their concerns. Many of them feel frustrated reporting into the CIO. I am fortunate in my role because I have direct communication with the Finance & Enterprise Risk Management Committee and attend every Board meeting. There is communication all the way up the ladder so effective governance can be applied as it relates to risk. This is an uncommon structure for an organization today, but I am lucky to have it."

BUY-IN AND COMMITMENT FROM THE BOARD FOR A NEW ENTERPRISE RISK PROGRAM

Nesgoda's team strategically created a risk assessment methodology and built out a comprehensive and effective enterprise risk management framework. "In introducing a risk management program, we started with a top down approach," Nesgoda explains. "We received buy-in from the CEO and Board-level committees, and we spoke with senior management. We explained our process and the changes to expect. We explained what management should expect from us in terms of risk."

NESGODA'S THOUGHTS ON CLOUD SECURITY

> We are leveraging the cloud and Web services. A big challenge for us is determining how we extend our security policies out to those vendors. We are looking at the CASB market, but it is still largely in its infancy. We will be using Office 365 and Microsoft has done a good job of documenting security controls, but we still need to ensure that it meets our specific security standards. A CASB can help with that.

A key to Sikorsky's risk management program is that each group in the organization is made aware of their own risks and what must be addressed. "We have regular meetings among executive leadership. In those meetings I, and my department, report risks by department, and then slice it further by risk category, such as reputational and strategic risk. This makes it easier for business executives to understand and react to risks," describes Nesgoda.

Rolling out this program constituted great effort for Nesgoda and his team. "We sat with project managers and subject matter experts and attempted to automate and streamline processes as much as possible. We leveraged an advanced vendor management process and we built a risk assessment questionnaire for all systems."

Now, risks are reported up to the Board on a regular basis. "If the Board sees high level risks they can ask further questions. The Board's attention to risk lends the program greater priority in the organization," says Nesgoda.

The Board asks a number of questions to Nesgoda as they work to understand the credit union's risk posture. Nesgoda comments, "For example, I'll present a risk assessment that may have an aggregate risk of medium, my chairman of the Board will say, 'Is that ok? What do we need to do about it?' Those are excellent questions. I explain, what we need to focus on is 'what are the gaps and what are we doing about them?' I'll explain this to them, then let them know the actions we need to take to mitigate a particular risk. Of course there is only so many resources to go around, so part of risk management is ranking projects by risk that need to be addressed. We put the most dollars to the highest risk priorities. That's the second most common question that I get from the Board - ranking the risks for remediation."

ALIGN WITH BUSINESS PRIORITIES TO IMPROVE SECURITY CONTROLS

Nesgoda and his team make certain their efforts stay aligned with Sikorsky's four main objectives, which are reinforced each year at strategic offsite planning meetings. "As an organization we have four objectives. They include financial stability, creating an effective workforce, building and protecting the credit union identity, and pursuing organizational excellence. We align all of our security and risk management initiatives to support these four business objectives," he explains.

To drive security programs forward with strategic business alignment, Nesgoda recommends other CISOs partner closely with business units. He comments, "Start by talking to business leaders and be proactive in communicating with them as they take on new applications. Ask, 'How can I help you move this project forward?' Be part of the project team from the beginning. This will allow you to bake security concerns and controls into the application while you help your colleagues solve their problems. Do not be the person who says everything is high risk, prioritize the risks for them and help them find solutions to mitigate those risks which helps them accomplish their objectives."

Nesgoda's security and risk program relies heavily on Managed Security Service Providers (MSSPs) and consultants. His dedicated security team is small. "With so many unfilled security jobs in the market, I know that it will be difficult to hire and retain the best resources, so I leverage consultants and MSSPs," says Nesgoda. Nesgoda also points out that his IT team is very security-aware and capable.

"We are focused on creating a more adaptive security architecture, and leveraging third party vendors to do so. We are strengthening our incident response program, so that is our big focus in 2017."