PROFILES IN *Confidence*

JOE CORSI

DEPUTY CISO
EXCELLUS BLUECROSS BLUESHIELD

HEADQUARTERS: Rochester, NY

EMPLOYEES: 3,500+

REVENUE: $6.6 Billion

Joe Corsi majored in Computer Science during college because he felt it was a forward leaning industry and something that would set him up for success in his career. After graduating, he worked in the US Army for seven years as an Officer. For the first four years he served as an airborne paratrooper before ultimately moving into the role of a Cyber Intelligence Officer assigned to US Army Cyber Command. He explains, "Getting into cybersecurity was exciting because the Army was just getting their feet wet from a security standpoint, so everyone was essentially learning together. We had very little internal training available at that time and therefore utilized content provided by third parties such as CompTIA, ISACA, and ISC2."

Early in his military career the Army provided many courses focused primarily on leadership. When Joe graduated US Army Ranger school he went through intense leadership training that helped refine his skills and prepare him for the next step of his career as a leader within the cybersecurity industry.

After leaving the Army, Joe began working within the cybersecurity team at Paychex Inc. where he quickly moved into leadership roles while gaining valuable tactical and strategic experience. After an opportunity at Excellus BlueCross BlueShield opened, Joe excitedly took on the Deputy CISO role, with a focus on identity management and security architecture while also supporting the overall security program.

THE ROLE OF A DEPUTY CISO

Joe says CISOs have become increasingly responsible for managing upwards by reporting to the C-suite and the board. He comments, "The role of a Deputy CISO is to assist in keeping the overall organization running efficiently whether that be assisting in the handling of major incidents or leading large staff events. A Deputy CISO is like having a Chief of Staff role within your organization. It's a valuable position and one that I believe helps keep the department moving forward when the CISO must focus on so many additional responsibilities related to the business."

According to Joe, Deputy CISOs gain vast experience working across all domains of cybersecurity and their core value is in assisting each area to allow the CISO to focus on larger strategic initiatives and executive reporting. His day-to-day work varies greatly, exposing him to all areas of security and business, from leading his own team initiatives to assisting in the preparation of board materials on behalf of the security organization.

MEASURING AND ASSESSING RISK

Joe believes measuring risk starts with using a well-documented framework and leveraging it to re-assess on a reoccurring basis. He says, "Governance, risk, and compliance is a significant portion of our organization responsible for maintenance of our policies and standards and takes the lead in managing our relationship with our external Audit, Legal, and Risk partners. One additional key component of this group is maintaining an accurate and up to date risk register utilizing industry-recognized terms and scoring. I don't think enough organizations utilize well-documented concepts such as Annualized Loss Expectancy (ALE) and Annual Rate of Occurrence (ARO) when determining the best ways to manage identified risks to the company. These concepts are helpful when trying to determine if the work to reduce an identified risk outweighs the costs that may occur if the risk is actually realized. Organizations also have a tendency to forget that you can also accept, transfer, and avoid risk which should all be options considered as part of the larger risk management process."

Joe says the primary value of continuously measuring risk

is that it helps cybersecurity teams remain focused on areas of most importance to the organization. With new projects and priorities popping up on a regular basis, it is important to ensure your finite resources are focused on areas of higher risk where reduction can occur in an effective manner.

SPEAKING IN BUSINESS TERMS

To effectively present and communicate with executives, Joe says there must be a balance of explaining clear and concise metrics while also utilizing some amount of active presentation skills. He explains, "Knowing how to convey what can sometimes be a complicated and nuanced technical thought to non-technical audiences can be incredibly difficult. I've seen senior leaders struggle when talking to other leaders outside IT about certain topics because they struggle to avoid technical terms or jargon. Ultimately you must be able to tie your points back to something your audience is familiar with such as business goals and objectives."

"I've seen senior leaders struggle when talking to other leaders outside IT about certain topics because they struggle to avoid technical terms or jargon. Ultimately you must be able to tie your points back to something your audience is familiar with such as business goals and objectives."

He continues, "Just as important as conveying a clear message is being concise and purposeful with your message. Your ideas can get lost, and you can find yourself being uninvited to meetings if you are seen as somebody who goes off-topic or conveys a long thought with no specific ideas for action. The goal is to have a seat at the table and maintain that seat. Even better if you can find yourself continuously requested to come back because they know it will be an important and well thought out message and a good use of their time. You are successful if you've appropriately communicated risk and achieved any desired outcomes relative to the audience whether that be for awareness or action."

CONTINUING TO GROW AND LEARN

Joe approaches leadership with a flexible mindset and core ability to adjust to the specific needs of those that he leads. When hiring, he focuses on finding individuals with a core set of values and a balance of soft and technical skills. He says, "If you give me somebody that is humble, hungry, and smart, I will find a place for them in my organization. That's not to say that technical skills aren't required in some areas. There are certainly positions within every security team that call for those talents. However, often I find myself looking for people that can communicate clearly and are self-starters that can get work done without having to be supervised. Once I've got a team of those people, the focus shifts towards making them comfortable within their core area of responsibility whether that be through mentorship, peer-review, or training. In my experience if you have individuals with a strong core set of soft skills, most are able to pick things up relatively quickly only a few months into the position regardless of previous experience."

For Joe, peer groups are an essential part of his growth and learning as a security leader. He comments, "Creating networks for information sharing can be seen as a force multiplier. No single organization has all the answers, best practices, tools, etc. If I'm struggling with a particular problem within my own group I know I have the option to reach out to ask others for help. Being able to quickly contact a trusted group of peers on a particular topic is extremely valuable. I can ask them which vendors and tools they prefer or if they've improved a particular process recently. Ultimately this helps me feel like I'm not in this on my own and ensures that I have support whenever needed. Giving back to the community is also important and I try to do that as often as I can."