PROFILES IN *Confidence*

JONATHAN SANCHEZ

CISO
TRC COMPANIES

HEADQUARTERS: Windsor, CT

EMPLOYEES: 6,000+

REVENUE: $1.5 Billion

Jonathan Sanchez is currently the CISO for TRC Companies, Inc., a global firm providing environmentally focused and digitally powered solutions across key markets which address local needs. Now over three years into his tenure, he has established strong communication between security and the business, built his team, and continued to reduce risk through a business-focused, strategic approach.

Jonathan's first role in security began as an intern at JP Morgan, where he worked on intrusion detection systems and data loss management projects. He quickly realized he had a knack for problem solving and was promoted to the global incident response team. He comments, "That's where the rubber really met the road. I already had the foundation built for cybersecurity within my previous role and moving up to incident response forces you to do everything from soup to nuts. Being a global team, we were on call 24/7, we built everything you could think and worked with teams globally to ensure that we were performing cyber correctly and continuing to pioneer the lead."

During his time at JP Morgan, he acquired an undergraduate and master's degree in Information Technology/Information Management from Syracuse University with certificates of advance study in Information Security and Telecommunication. After spending five years at JP Morgan, Jonathan moved to BNY Mellon to help them develop their cyber department, growing the team from eight to over 150 people, and increasing security maturity. After three years, he decided to leave the highly regulating banking world and move to TRC Companies, Inc.

COMMUNICATING IN BUSINESS TERMS

Jonathan believes successful CISOs align themselves to the business and are able to clearly articulate the financial impact of security. He says, "Being able to speak in terms that executives and the board understand is important. Leaders receive information in different ways but the key to successfully communicating is by understanding your audience. Boards deal in business terms, management terms and financial terms. You have to be able to communicate that cyber incidents can lead to the firm potentially losing millions of dollars. This is what gets their attention. Cybersecurity doesn't make money as it's not a revenue generating function; however it saves money and money saved is value earned. The board understands what risk is and its potential impact, but until you help them understand what it means to the bottom line or from a cost perspective, they don't easily associate or simulate what it is from a one-to-one perspective. Cybersecurity can be a costly function but being able to right size investments and provide ROI's by deploying cyber solutions, business functionality and uptime are enhanced."

Jonathan says it is vital to show KPIs and metrics that demonstrate how cyber is aiding the business and the maturity of the overall program, and resiliency in responding to potential threat actors. Having these types of metrics demonstrates improvements over time and highlights areas of weakness and strength. Presenting to the boards and executive audiences will require a mixture strategy document, revealing overall strategy, potential key threat areas to mitigate risks and threats identified. Additionally, including visuals for the executive dashboard, which leverages RAG (Red, Amber & Green) rating indicators helps provide awareness from a criticality perspective.

RESPONSIBILITIES

Anything cyber-related falls under Jonathan's umbrella of responsibilities. Part of his role is overseeing their internal controls, how they manage employees and the data they have access to, as well as external risk management and third-party governance and compliance. Jonathan believes data is the lifeblood of the organization and spends time working with the business to determine if the right controls are in place around how data is being used. He says, "I spend a lot of time working with the business and understanding what they're doing with some of the data to ensure that we have the correct cybersecurity provisions to manage data from a threat perspective. We make sure we understand where the data is living - at rest or in movement, and how to securely transfer to make it available to clients or project party

members that are outside of our organization."

Vulnerability management also sits under Jonathan, an area his team focuses on, especially as it relates to reducing the risk landscape. His team also manages incident response and digital forensics by holistically managing any incidents. Another area of responsibility is mergers and acquisitions. He explains, "Whenever we're evaluating the possibility of looking to expand by acquisition, I'm responsible for evaluating their cyber posture, the company data and understanding the potential risk to our organization. There's a lot of due diligence required to ensure it is done correctly before providing any type of signoff and commit to moving forward."

Jonathan and his team are also involved in digital innovations, especially as it relates to building applications. Security must assess risk around application development and ensure mitigating controls are in place to maintain strong security posture with layered defenses.

In terms of the most current focus area, investing in cybersecurity awareness and training is paramount for Jonathan to maintain a strong cyber posture. He comments, "People are your top asset, but they're also your biggest risk. Understanding cyber risks are important but understanding user experience and their interactions with the environment are where the biggest risks are faced. Arming your users with the appropriate tools, knowledge and technology is only half the battle since vulnerabilities are exploited typically due to human error or oversight."

He continues, "Being able to manage the synergies between people, process and technology when addressing cyber threats are all equally important. No system is perfect, but you must have policies, process, and standards in place, which help guide users but also educate and train employees on best practices, while the right technologies are deployed to provide a safe and secure environment. We spend a lot of time training our employees to keep them safe from things like phishing attempts. Being able to train your users and make them aware of what they're up against or what they should be seeing makes it a lot easier for them to make the right decision. We put metrics in place from a baseline perspective, or phishing click rate, so we continue to improve our efforts to drive down the potential risk exposure."

ASSESSING RISK

Jonathan says risks vary across a widespread spectrum, so it is critical for security leaders to understand the different types of attacks and the controls in place to help mitigate or protect the organization. He explains, "Security isn't a one-stop shop, it requires continuous evolution and diligence, so it is important to revisit your controls, cyber strategy, systems, operations and internal alignment goals to keep pace with the growing risk landscape. Attacks are becoming more sophisticated, therefore being able to think like an adversary helps with your ability to strategize and protect your company's assets. CISO's not only need to focus on risks which are currently applicable but being able to be proactively prepare not only for local threats but situationally being aware of risks which can impact business due to current events."

He continues, "Organizations could face 90 to 1,000 risks, but are each and every one of those really pertinent to your organization? If you take a step back and you wrap up all the possible issues and systems together with your strategy, it will help you articulate what your current risk climate looks like, or what you're being faced with compared with the actual internal resources you have in your possession to help fight the good fight."

To do this effectively, Jonathan believes it is imperative to understand qualitative risk analysis. This approach helps to understand the critically of an impact from a financial and risk perspective. It focuses on measuring the likelihood and the impact to determine severity, then recording the results in a matrix. The matrix helps communicate the overall risk profile to the board and business executives. The overall risk profile to the organization provides cybersecurity maturity and preparedness.

Jonathan explains, "We try to do a yearly assessment for TRC and a full sweep with our penetration testing as well, to ensure that we're managing our network and understand what we're up against. We have moved to a quarterly evaluation from a control perspective to understand where we are seeing vulnerabilities. It helps us understand what we can do better to ward off bad actors and eliminate traffic from high-risk areas. We also have bi-annual audits internally to make sure that we're managing permissions and access controls efficiently. For example, we need to be able to track and monitor if a user internally transfers, therefore we'll need to re-provision their access, because risk happens at all levels, it just depends on how much risk you're willing to absorb and how you plan to manage it. Users are your top asset but biggest threat and at times don't even realize they have made a mistake."

GROWING AND DEVELOPING AS A LEADER

Jonathan says, "Cybersecurity requires commitment and passion to growing within an ever-evolving industry. The fascinating part about working in cybersecurity besides the potential to either keep you up late or get you up early is that there will never be a dull moment. In order to be successful, it requires dedication to your craft, willingness to learn and the ability to be flexible. Managing cyber events requires strong use of communication, coupled with soft skills and the ability to work as a team under duress. Outside of the everyday work activities, which can require you to become an SME (Subject Matter Expert), I think its critical for all cyber employees to stay relevant, attend conferences and successfully acquire relevant certifications."

To grow as a leader, Jonathan attends conferences and believes in the value of learning about niche topics, new cutting-edge technologies and coming trends. He says, "I'm currently in the process of working towards two new industry leading certifications. I personally enjoy attending conferences focused on specific topics with fellow CISO's and attending roundtables to discuss trends seen in the wild."