JOHN MANDRACCHIA

CISO
HEALTH PLANS, INC.

HEADQUARTERS: Westborough, MA

EMPLOYEES: 350+

REVENUE: $100.59 Million

John Mandracchia began his career working in IT as a second shift help desk employee at a local hospital in his early 20s. This early exposure to IT and the many components of working in that field, greatly interested Mandracchia and he continued to pursue IT as his career. Throughout his work in IT, he saw an emergence of work related to cybersecurity and eventually grew his career into that space. After working in various IT and security roles at hospitals, he then began working at Health Plans Inc (HPI), a third-party health plan administrator.

He explains, "I started at HPI in 2008. I had a career advancement opportunity that became available. I'd been at my previous company for 11 years. I loved it there as well, but with HPI, I fell in love with the organization because it was a smaller organization that allowed us to have exposure to a lot of different components that I hadn't had with larger organizations. The people that I work with are friendly, it's a diverse organization and everyone's so hard working, so it's kept me there for so long."

> *"...with HPI, I fell in love with the organization because it was a smaller organization that allowed us to have exposure to a lot of different components that I hadn't had with larger organizations."*

He began his work at HPI as a Systems Engineer and transitioned into a Team Leader for System and Infrastructure before taking on the CISO role in 2020. He says moving into a C-level role meant shifting away from being heavily focused on the technical day-to-day in order to address the managerial requirements as a business leader.

Mandracchia is responsible for protecting the confidentiality of PHI and PII while aligning security with the business. As with many smaller organizations, he wears many hats which include overseeing both the cybersecurity and infrastructure groups.

LEVERAGING THE CIA TRIAD

Mandracchia leverages the CIA triad of confidentiality, integrity, and availability of data to continue to strengthen his security program. By focusing on these key areas, Mandracchia implements high-level strategies that his team expands and executes on. He comments "A sub strategy of confidentiality could be to improve access control. A sub strategy of availability could be to mitigate something like a DoS vulnerability. Concentrating on these high-level methods have proven pretty well for me at HPI."

One of Mandracchia' s specific strategies for 2021 is to continue to strengthen their endpoints. He says because they are not working with just business computers or business networks anymore, their applications are becoming device agnostic and expanding across many networks. It is important for him to make sure the multitude of paths that lead to their data is manageable and secure.

In order to communicate the value of investing in endpoint protection, Mandracchia focuses on discussing risk with HPI's executives. He says, "It's a lot of risk evaluation and weighting risk. If there's multiple components to our network, we go through them and pinpoint the ones we feel are becoming higher risk. We communicate that process by going back into our risk assessment process and showing why we think something has changed. We're expanding desktops, we're making applications device agnostic, we need to make sure that we can portray that on paper, the increase in risk."

Like many other security programs, Mandracchia says resources are often a key challenge. He explains, "Similar to how real estate is location, location, location, for us it's resources, resources, resources. I define resources as employees, equipment, skills, experience, utilization of products, services, and so on. Where I work at HPI, the organization has had continuous growth year after year, and with that growth, you have a demand for increase with those resources. But the challenge with growing efficiently is to address those growth demands while keeping costs manageable so you can keep being competitive in a competitive market."

SHIFTING PRIORITIES

Mandracchia says their disaster recovery plan helped them through the many changes brought about by 2020. The strong plan in place with their disaster recovery program provided a framework to easily adapt to dramatic changes, such as those that sprang up with a newly remote workforce. He remarks, "I'm fortunate to report to our CIO, who I've been working with for 13 years, and we've always gone through every connection possible from switches onsite, routers onsite, network connections, everything is pretty much redundant. We always try to have a fail over plan. All of our employees from day one of the pandemic were working remotely and of course we had some issues with connectivity, stuff like that, but really the biggest change that we noticed was the communication demand."

This communication change required their organization to identify how they can continue to stay in touch in a productive and efficient manner. Mandracchia states, "We realized Microsoft Teams is pretty much a front facing application for all of the Microsoft products and since we're heavily a Microsoft shop we saw it as a win-win and we could eliminate our costs for Zoom and GoToMeeting. Now it is how do we implement it? How do we utilize it? How do we make sure people aren't going to over-utilize it and put PHI on there? It took us a little while to get the Teams platform implemented but as I said, we immediately recognized there was value for it, but getting it in place was the priority."

"Similar to how real estate is location, location, location, for us it's resources, resources, resources. I define resources as employees, equipment, skills, experience, utilization of products, services, and so on..."

PHI AND THE CONSIDERATION FOR DATA

In the PHI protection industry, including healthcare, health insurance, and other related entities, Mandracchia says becoming more granular with data identification will only become more important and prevalent. He comments, "We're seeing such a rise in regulations and regulating bodies such as GDPR and CCPA. Health Plans is a company that started in New England and is looking to expand nationally. And as we expand nationally these regulations are going to be prevalent. And the regulations are very aggressive when it comes to being very specific with items like data mapping. It's not only being able to map data and map the flow of your data, but the ability to carve out any single person, certain attributes of a person, pretty much at the request of the customer."

They must ensure their data is mapped well with an ability to focus on cherry picking exactly what they want to remove from data, wherever it resides. Mandracchia says the challenge is there may be legacy systems or smaller level SaaS providers that cannot autonomously sift through legacy data with a command or script to remove the individual or attribute.

INSIDER THREAT

Mandracchia says it does not take a technically minded individual to penetrate an organization and become an internal threat in today's world. Employers must extend a level of trust to their employees and also place the right controls in place, such as strong access controls, damage may be minimized, according to Mandracchia. He continues, "The simple fact remains that if anybody who has a camera, which is widely accessible, can capture data and extract that data, it's not that difficult to achieve. I can't speak as to why there would be a rise in insider threats themselves, that would be pure speculation, but I can say that it's a concern and it should be a concern for most organizations."