PROFILES IN Confidence

JOHN MANDRACCHIA

CISO

Health Plans Inc.

HEADQUARTERS: Westborough, MA

EMPLOYEES: 500+

REVENUE: $74 Million

John Mandracchia was originally featured in the Feats of Strength magazine in March 2021, where we profiled his career experience, goals, challenges, and focus areas. Since then, he has significantly grown his skillset, evolved his approach to leading an information security team, and ensured he stays up to date with current threats impacting both his organization and the healthcare industry as a whole.

John began his career at Health Plans, Inc. over sixteen years ago, working his way from System Engineer to his current role of CISO, a title he has held for almost six years. Health Plans, Inc. is a national third party administrator of customized, self-funded health plans serving employers and brokers. John brings over twenty years of experience in cybersecurity and infrastructure to continually help the organization accomplish their goals and serve their customers with quality services. John's success stems from his focus on core competencies including strategic cybersecurity planning, implementing risk management policies, and leading cross-departmental process improvements.

RANSOMWARE AND SUPPLY CHAIN SECURITY

When discussing new challenges that have surfaced since we last spoke with John, he shared that ransomware and supply chain security have become incredibly relevant areas of focus. He explains, "There's been a significant uptick of ransomware attacks, especially in the industry of healthcare-related services. It is a consistent threat to environments that carry highly sensitive information and working in any healthcare related fields makes you a prime target. We focus on supply chain and ransomware attack defense because, as the saying goes, you're only as strong as your weakest link. Social engineering attacks have become very sophisticated and it is a lot easier to fool unsuspecting individuals. It only takes one employee from one vendor we supply data to, with an off day, for us to be impacted."

He continues, "I've focused on how we can evaluate the security postures of the vendors around us and how we can work with them. When we do this, we don't expect everyone to have fortune 10 security levels or have military grade defense mechanisms in place, but we are ensuring these vendor organizations are aligned with NIST, have SOC validations, or HITRUST certifications. Positions such as these are really assuring to us as an organization. We like to see that our vendors are putting these types of controls in place, it gives us peace of mind."

Having a comprehensive plan against ransomware and supply chain attacks is paramount for John and his security team. They not only need strong policies in place, but they must continually research and stay one step ahead of current threats or changes as it relates to these areas.

PROACTIVE SECURITY AROUND AI

Artificial Intelligence is a large area of focus for not only John and his team, but for the organization as a whole. He shares, "We are looking at ways that we can use AI to help us without reinventing the wheel. In the short term, AI can act as an assistant to improve efficiencies, and in the long term, it can help us improve functionality across the organization. From a security perspective, it is our role to better

> *"From a security perspective, it is our role to better understand how AI might be used to damage the organization. Deep fakes and the capabilities of voice cloning are something of great concern."*

understand how AI might be used to damage the organization. Deep fakes and the capabilities of voice cloning are something of great concern. It is scary to think about how these realities might be used against us. So, it is important for us to fully understand how AI can be used, and how we can create awareness and education around it so we can defend against it."

It is also important for John to help his organization securely implement their AI objectives and align AI best practices with their priorities. The goal is for security to help streamline proactively and ensure they are educating along the way.

STRONG DATA GOVERNANCE

According to John, the fundamental pillar of a strong data governance program is implementing the correct controls and tools to identify data types. He comments, "Data governance starts with the proper identification of data attributes such as data type and how old the data is. This process allows for lean data retention. There are some great tools that help detect the type of information in certain data, so you can identify where PHI or financial data resides and monitor it according to policies you have set. These policies should outline data retention, data destruction, and usage to ensure the right actions are taking place based on the type of data present."

Automating the identification of data is a key component of this process. Through this automation, the organization can save time and ensure data is properly identified.

John believes AI will expand and continue to significantly impact data governance. He explains, "It simply makes sense that there will be a heavier AI integration process when it comes to governing data. In the past I would spell check an email by hitting F7 prior to hitting send, but now we have AI that's reading our text in real time and telling us how to improve our sentence structure. So, for data governance, if we can invoke AI to assist the user and automatically classify data, then less manual work must be done. I see a lot of growth potential in this area."

GROWING AND LEARNING

Surrounding yourself with great people that want to learn is John's motto when it comes to leading a mature and proactive security program. To consistently build a strong team, he ensures he provides a platform for success tailored to each member's personality. For example, if he has an employee that prefers to speak in depth strategically, he gives them the time and space to do so.

John continues to engage in networking with his security peers on a regular basis. He comments, "Through attending conferences and networking events, I meet people that are in similar situations to me, and it's really reassuring to know they are facing some of the same challenges. To know I'm not the only one dealing with these things is nice, but also helpful to learn from them on how they overcome it. I gain a lot of value in conversations that talk about the frameworks people are following, even from a nuts-and-bolts perspective when talking about granular controls they have implemented."

> *"Through attending conferences and networking events, I meet people that are in similar situations to me, and it's really reassuring to know they are facing some of the same challenges."*

To grow his skillset, not only does John read industry publications and journals as time permits, but he finds a lot of value in listening to cyber podcasts that provide short, tangible information on an almost daily basis. He recommends other CISOs to glean industry information in whatever format works best for their schedules.