

# MATT CERNY

## DIRECTOR OF CYBER SECURITY INTEGRA LIFESCIENCES



**HEADQUARTERS:** Princeton, NJ

**EMPLOYEES:** 1,200+

**REVENUE:** Private Company

Matt Cerny began his career in security over 20 years ago, with a vast amount of cybersecurity expertise along with 10 years of experience in infrastructure. As an avid contributor to the industry, Matt participates in a number of security communities that champion peer networking and growth. He currently works as the Director of Cyber Security at Integra LifeSciences, a medical technology organization.

When talking about his first introduction to security, Matt shares, “The reason I got into cyber security was that the company I was applying at was looking for someone who could perform security for Windows, Linux and AS 400. They were looking for somebody with a skillset that wasn’t just isolated into one particular platform, but who had knowledge of multiple platforms to be able perform the integration between those three entities. So, I took the knowledge I had gained through my career to look at those three different operating systems, understand the integration and apply security foundations to them. That is how I came into security, and back then security was not as big of an area of focus, it was a lot of access control and identity work that ultimately morphed into the broader scope of what security is today. I’ve been able to see the growth that has taken place over the last 20 years.”

Working at Integra LifeSciences has been incredibly rewarding for Matt, because he has an opportunity to not only fine tune and flex his skills every day, but the work he does impacts the company’s overall goal of improving lives. Integra’s vision is to expand access to promising technology that enables the body to regenerate damaged or diseased tissue. Grounded on this vision, the company revolutionized the field of regenerative medicine and has since grown to be a leading global provider of neurosurgical solutions, regenerative technologies, and surgical instrumentation ([www.Integralife.com](http://www.Integralife.com)).

In his role as Director of Cyber Security, Matt’s responsibilities span globally as they have offices and manufacturing facilities around the world. His team is responsible for security operations as it relates to cyber risk reduction and cyber risk management, and also includes identity and access management and operational technology cyber security. Matt comments, “The way I perceive cybersecurity is by relating it to a submarine. If a submarine were hit by a missile, in a figurative manner, we, the security team, would be able to shut down that particular hole that was hit and the ship would still function while we made the necessary repairs. You’re protecting certain areas of the submarine, in order to cordon an impacted part of the ship, but to also make sure you are still able to operate and continue on.”

### FOCUS ON AUTOMATION AND THREATS

Looking towards the next year, Matt is focused on several core areas to improve the overall security program and continue to reduce risk. Automation is top of mind, and their goal is to establish a methodology to reinforce or test one control that could ultimately comply to multiple regulations. For example, if testing multifactor authentication, they would be able to look at how many frameworks or regulations would that adhere to, so they can holistically apply it to the relevant areas across frameworks. The outputs might show that they are 80% in compliance with one framework, and only 60% compliant with another. The concept of a unified

---

*“I moved over to Renaissance because it looked like a great experience for me, leadership was switched on to the benefits of security, I was able to work in the education industry and it was clear security had support from the board.”*

---

compliance framework is a top priority, something that will help his team save valuable time and resources. To accomplish they are engaged with outside help to implement changes and integrate this methodology to match the needs of their security program.

Managing and understanding threats is another focus area for the Matt, specifically as it relates to the human element of security. He says, "Threat actors have evolved, take for example push notification fatigue, where one individual keeps receiving push notifications for multifactor authentication and ends up saying yes just to make them stop. It is security's job to ensure people across the organization understand that security is consistently evolving and just because we deployed one particular technology, that the problem may not always be completely fixed. SMS texting for multifactor authentication was common, but it is becoming less secure and the recommendation is to remove it. Now you might need to ask people to re-enroll in a new version of multifactor authentication and they might not understand why. It is our duty to ensure people understand that threat actors are changing, and our controls have to evolve alongside them to make sure we are protected. I think when it really comes down to it, people still play a very important factor in the adoption of cyber security as well as in the resiliency and the ability to recover."

## STAYING EDUCATED AND LEADING BY EXAMPLE

Matt believes in continuous education in order to stay ahead of trends and changes in the industry, but also to ensure they remain up to date on threat actors. He always tells his team to carve out some time in their day or week to focus on areas such as emerging technology in the industry, or other areas they are personally interested. He encourages his teammates to be constant learners, to always think about their career trajectories and work on skills to elevate their industry knowledge, whether it's broad areas or something more specialized.

Not only does Matt encourage his team to educate themselves, but he does so himself in a number of purposeful ways. He likes to spend at least 45 minutes reading during the morning. Whether it is intelligence briefings or gaining insight into the industry through various types of publications, he finds dedicating time to improving his leadership, technical or soft skills incredibly valuable. Networking with his peers is also very important to Matt, he sees tremendous value in discussing challenges or use cases with them, to not only share his successes but learn from others. Whether it is technologies they are evaluating, frameworks they are trying to align to, or any other relevant area, there is always something to be gained from hearing what your peers are going through.

---

## DATA GOVERNANCE

*"Data governance is really a partnership. There's a strategic aspect between legal, compliance and security on the leadership side of things. And then there's the tactical aspect of us learning from the data stores or the data owners. We're not experts in data, and I don't think we should ever pretend to be. I think this goes back to the people aspect of learning from the folks that are utilizing the data and it's really a partnership in that realm, right? As the strategic implementers or governors of the data, we have to approach the data owners and understand what their responsibilities are and what they are doing with the data. It's really this give and take of what the expectations are because at the end of the day, they're going to know what's best for what the data is utilized for. At the same time, compliance data privacy, data protection, and data security are setting barriers and foundations for the data. Also, we often overlook the role of artificial intelligence. I think a lot of people are playing catch up to go back and create these two-way relationships, yet companies that created them from the beginning are probably doing better on the artificial intelligence side of things. The fear is that once you introduce artificial intelligence, it's going to look across the boundaries of your data and maybe pull back things that you didn't necessarily want it to. Good data governance is going to set the tone for how well you're doing from an AI perspective as you continue to grow."*

---