SUE BERGAMO

GLOBAL CIO & CISO
EPISERVER

HEADQUARTERS: Nashua, NH

EMPLOYEES: 800+

REVENUE: Undisclosed

Sue Bergamo is currently the Global CIO & CISO at Episerver, a computer software organization offering a content management and commerce platform powered by AI-backed data and personalization tools. Bergamo works alongside executive management and a worldwide team of business resources, developers and infrastructure engineers, to deliver secure and innovative solutions within Episerver's data centers and cloud services. She is responsible for creating and executing on a global IT and Security strategy, as well as operating as a hands-on business and systems architect to develop mission critical solutions. Notably, Bergamo led industry compliance initiatives in ISO 27001 and GDPR.

EVOLVING INTO A CIO AND CISO

Bergamo says September 11th put cybersecurity in more of a pivotal position, when many people began to realize not everyone sitting behind a computer had good intentions. She saw an escalation of cyber-attacks, with a growing uptick not seen prior to 2011. This sparked many organizations to begin to see the need for a CISO and a heavier focus on protecting their organizations from a cyber perspective.

She says, "The CIO continued to have to provide security services for their companies. They started going in front of boards to make sure that companies were secure and that the board members understood how secure the company was. We put ourselves on the line. We had to ask for investments where there may not have been some or not enough in the past."

Bergamo says as the world continued to turn from a security standpoint, the different cyber hacks and attacks started getting more malicious and frequent. At the same time, additional software and vendors were coming into the marketplace with different toolsets, and it did not matter what role you had in security or IT, you could not help but realize security needed to be a component of your job.

To address this heavy shift of focus onto cybersecurity, Bergamo challenged herself to get a Master's degree in Cyber with a minor in International Terrorism to formally educate herself on the growing industry. She explains, "That has lended me very well, not just having the credentials, but combining the education with the on-the-job experience. This has led me to branch out and get a role as a CIO and a CISO and combine both pieces of that into one really terrific global company."

FOCUS ON SECURITY BASICS

"Getting attacked is a constant stream, but it's the defending around those attacks that makes us good CISOs, and again, protecting our company and protecting our employees. When this pandemic hit, I was talking to my peers about three types of companies out there. There were those that were prepared, those that were semi-prepared and those that weren't prepared at all. Those in the latter category are really in a world of hurt right now," comments Sue.

With cyber-attacks on the rise in the current environment, Sue says going back to the basics is around making sure we are protecting ourselves and spending time to make sure there are no holes in the environment that a cyber criminal can crack through. She believes it goes beyond network and infrastructure, that it is also about employees.

Many employees are currently working from home, with additional pressures outside of work, making them more vulnerable or distracted to engage in risky behavior such as clicking on a phishing attempt. She explains, "I think that getting back to the basics right now is around making sure that you don't have any holes in your environment. We must ensure we are not taking our foot off the pedal with educating our consumers, employees, and spheres of influence on the importance of staying vigilant and focused on protecting ourselves because unfortunately cybercriminals are not on holiday."

She continues, "I think these devices, laptops, desktops, whatever you have in front of you, are the most vulnerable right now, especially from a work at home standpoint. As a CIO and CISO, I make sure that our endpoints are protected. I have employees all around the globe, I can't support all routers in everyone's home. No one can. So you have to make sure that your employees are educated on how to configure a router as best as possible to make sure that it's encrypted, to make sure that it's not open and noticed from criminals that are hanging around, and that it's locked down and protected through a key. That's just step one. It's the device, the most vulnerable piece of the puzzle, that's where things get in."

Bergamo says the next part is making sure your network is protected and you have a strong handle on your security posture. She says it is important to ask yourself – does the data center have its own disaster recovery plan? What does that do for your business if they are hacked? Is there enough software in place to make sure that firewalls are protected? If you're a company that's sitting on the cloud, are your applications protected? She believes if you identify anything missing from these types of questions, then you must shore up and close gaps as best as possible.

EDUCATING EMPLOYEES

Bergamo is focused on educating her workforce and community on proper safety. She explains, "From a physical standpoint there are some nations out there that you're not supposed to leave your house. That's not necessarily a cyber issue, but it is a security issue. If you're at home and you have multiple people using the device, maybe your company didn't let you bring a laptop home, maybe you're VPN'ing in or you're using your Wi-Fi. There's many different types of scenarios. How to protect yourself in a connection first and foremost, how to make sure that your device, no matter what you're using, is protected."

> *"Getting attacked is a constant stream, but it's the defending around those attacks that makes us good CISOs, and again, protecting our company and protecting our employees."*

Bergamo says there are many different nuances in this situation along with a variety of risk factors. Since the most vulnerable component of working from home is the laptop, you must ensure you are upgrading and using a password, among other considerations.

She comments, "With many vendors and tools that are out there, as soon as a new signature file is identified, they'll push it down to you. There are environments that don't have those pushes and you have to keep up with them on your own, that means you have to constantly remind people to do so."

INVESTING IN NEW TECHNOLOGY

Bergamo believes before investing in a new technology, you must engage in strategic requirements gathering to ensure it meets key standards. She explains, "What are your security standards? What kind of information are you looking for? It's about understanding what the standards are and how you satisfy those standards to meet the needs. And then from a requirement standpoint, you fulfill those needs and then figure out what's the next step of picking the technology. You must have to have a clear set of criteria involved in order to pick technology."