**Cyber Security Business - Episode 12: "Back to Basics"**

**with Sue Bergamo, CIO & CISO, Episerver**

**KATIE HAUG**: Hello everyone and welcome to Cybersecurity Business. I'm Katie Haug filling in for our regular host Kevin Pouche, so thank you for listening to me provide the interview today. For those of you who are new to our podcast, we interview CISOs and other security leaders to hear their advice about the business of information security. And our goal is really to give our listeners actionable takeaways so that they can increase the effectiveness of their security programs. Today I'm very excited about our topic. We're going to be discussing what getting back to the basics means for CISOs. I'm joined by Sue Bergamo, the CISO and CIO at Episerver, a global eCommerce company headquartered in New Hampshire. And this is actually Sue’s second time on our podcast, so welcome back and thank you again for joining us.

**SUE BERGAMO**: Thank you Katie. Thank you for having me again.

**KH**: So to kick it off, I'd love for you to share with our listeners when you were first interested in information security and really how your career has evolved since then.

**SB**: That's a great question. I've been a CIO for a long period of time and security is always a part of the role, but years ago it wasn't really given the exposure as it has been today. I think what really set it off for the industry, at least in my mind is September 11th. We as CIOs, we kind of had to stand back as the rest of the world did too. And really for the first time in our lives think, the people that are sitting behind computers, they don't always have good intentions. And from there I personally saw an escalation of cyber attacks, more so than years earlier to 2011.

There were a few things, malware, viruses as we used to call them back then. But cybersecurity really took off and the CISO role became something that most companies decided they needed, or at least those that started to be very interested in security. 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. And everyone really stood up and took attention. As the world continued to turn from a security standpoint, the different cyber hacks and attacks started getting more malicious, more frequent.

There was more software that was coming out in the marketplace, more vendors that were coming out in the marketplace with different tool sets and it didn't matter what role you had in security or I should say in IT, you couldn't help but realize that security needed to be a component of your job that you'd better really start paying attention to. Talking with a lot of peers, industry presentations, speaking with people in other companies. The attacks became more frequent and it was almost like it was an invisible fight. How do you fight something when you can't see it? We're all there trying to protect our networks and our servers, but it went so far beyond that.

From a career perspective, I would say that as the intensity continued to increase with cyber attacks and you started talking with more people, more companies, more vendors, and considering more holes in your own infrastructure and your own environments, you had to really take it very seriously in general and just sort of pick, what's your flavor of the day? Is it malicious attacks on email? Is it your network? As these attacks increased, it just became more and more so, I don't consider security just around cyber, it's so much more. It's physical attacks. We see that in the United States, we have active shooters all the time, right? So it goes the gambit. And CISOs need to be concerned about not only software or environments and infrastructure, but people, their employees and the people that visit, and physical security. It's a never ending list. It never changes. It just keeps getting more intense.

For me personally, I challenged myself to get educated in addition to what I was doing on the job and I decided to get a second master's degree in cyber, but this time I did it with a little flair and got a minor in international terrorism so I could be extremely well educated on what was going on out there. That has lended me very well, not just having the credentials, but combining the education with the on the job experience has led me to branch out and be able to get a role as a CIO and a CISO and be able to combine both pieces of that into one really terrific global company. So that's sort of my story. You come up through the ranks when you've been around the block a few times and you get educated as things happen and then you say to yourself like any good CISO should be saying to themselves, I'm not going to be reactive. I'm going to be proactive and make sure that my company is secure.

**KW**: What are your top priorities for the next 12 months? Many CISOs are focusing on foundational security principles. What does getting back to the basics mean to you?

**SB**: That's a great question. I would like to start by saying that foundationally, mature businesses have a good security posture, we need to in this day and age. Getting attacked, it's 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, there's really 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.

And unfortunately many of them have shuttered and that's not just around security, it's how we're doing business today. But businesses are vulnerable right now. The world is hurting and you'd like to think that cyber crime would be decreasing. But that's not the case, there's an influx of attacks, there's an influx of malicious attempts on employees, people in general. It's really unfortunate. I think that going back to basics is around making sure that we're all protecting ourselves and really spending the time to make sure that we don't have any holes in our environments that a cyber criminal can crack through.

And that's not just network. It's not just infrastructure, it's also employees. People are not really paying attention today. They've got so much on their minds. They're working from home. They may have a kid sitting on their lap, they may have an elderly parent who's been infected with this virus or just sick in general, and they're not paying attention. They're clicking away and they're multitasking and things are coming their way and I hear it all the time, people are answering questions either through vishing or phishing attempts and then they stop what they're doing and they go, oh my God I probably shouldn't have done that. So I think that getting back to the basics right now is around making sure that you don't have any holes in your environment and making sure that you're not taking your foot off the pedal with educating your consumers, your employees, your sphere of influence on the importance staying vigilant and staying focused on protecting yourself in this environment because unfortunately cybercriminals are not on holiday.

**KH**: How can those unprepared companies start to make sure that they don't have any holes in their environment? What does that mean for them? What actions should they take and what are the steps that they should take to really get those basic foundational principles to avoid having those holes in the environment?

**SB**: There's a couple of ways that you can handle it. If you weren't prepared for the pandemic, which meant you didn't have a business continuity plan in place, it's too late, right? It's too late. So you've got to get up and running so that your business can get back up and running again. If you don't have the means or if you don't have the skills and the expertise in your group, go out and find someone who does. But don't just take the first company that comes along, interview three to five companies. Make sure that you're comfortable with what you're going to hire. Then I think you have to look at it from the standpoint of, we all have an end point device.

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. So, you know, 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 of those 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.

The next part of that is within your network. Let's say you're back in the office or even if you're remote working from the office, making sure that your network, your data centers are protected. What's your security posture? Even in this pandemic, your data center, does it have its own disaster recovery plan? Does it have a BCP for itself? If it doesn't, what does that do for your business if they are hacked? And then looking at your physical infrastructure in how you're monitoring and logging for events and alerts.

Do you have enough software in place to make sure that your firewalls are protected, your servers are protected, you just start taking it piece by piece by piece and identifying any gaps. And then you raise it to the next level. If you're a company that's sitting on the cloud, are your applications protected? Are you developing for security? Are you testing those applications for security? Is your infrastructure within a cloud environment, no matter if it's IaaS, PaaS or SaaS, is it protected? Have you done the right things either in a single or a multitenant environment to make sure that the infrastructure is geared from a security posture.

And if you see that any one of those things, in either one of those levels isn't protected, then you have to go back and you have to shore it up and close those gaps as best as possible. And unfortunately for companies that didn't prepare in a pandemic, this is a disaster. It's a global disaster. Tomorrow can't come soon enough. Yesterday came too late. You're not prepared. You're going to need help and you're going to need help pretty quickly to get your business back up and running. So my advice would be go hire someone if you don't have it.

**KH**: And you mentioned educating employees is one of the initial steps to take along with educating them on how to configure a router. What are some of the other things CISOs should be educating their remote workforces on right now?

**SB**: Believe it or not, I'm spending a lot of time educating people on community and government, situations around the pandemic and the orders, so 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 your VPN’ing in or you're using your wifi and maybe you're not using VPN. There's all 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.

It's as easy as antivirus software on your device. If you're letting your kids head off to some internet game, or God forbid they're clicking on some advertisement within a virtual room. What are they doing to your PC? And again I'm making the assumption here that they're not using a company sponsored PC to play games with. They're using it on their own device from home. So it's all of these different nuances and different risk factors that you have to continue to say to people, if you're going to come into the company and process information, you have to make sure you know what's happening on your own device and make sure that that device is protected.

I still think it goes back to the most vulnerable component of working from home, which is your laptop, the device that you're on every single day. Zoom, right? It's not just zoom. They did get a little bit of bad advertisement, for people that didn't know how to use a UC tool correctly. When you have an open meeting and it's not password protected and you're not asking people to log in, it's open. It's like an open connection on the internet and anyone who's savvy enough to get through can do so, these are some of the things that you have to harden in your own network. You have to follow the vendors recommended ways of using their software. If they ask you to upgrade, upgrade, if they ask you to use a password to protect the session, the software, whatever.

And these are things that you have to consider. One thing that I was just thinking about this morning, Mac devices, to give Apple a little poke in the eye, everyone thinks oh, we don't get infected. Well they do. Mac devices in the enterprise are really hard to have because there's no real way to push software down. The users have to make sure that they're going out and looking for those upgrades, either operating system or anti viral. You have to constantly remind them, make sure that you're clicking and upgrading often. Because with the other vendors and with the tools that are out there, as soon as a new signature file is identified, they'll push it down to you. These 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.

**KH**: And a lot of these CISOs are rapidly identifying where the gaps are and how can I fill them and how can I also focus on basic foundational security. So for a lot of these CISOs, how should they approach purchasing new technology while still focusing on foundational, basic security?

**SB**: This is an interesting question. If you have good methodology in your own environment, then I don't see too much of a difference in picking technology when you're in the office versus not being in the office working remotely. And what I mean by that, from a process standpoint, you should be vetting new technology the way you typically do, I may be of a different breed here, but technology isn't something that you just say, well, I like the new shiny toy and let me buy it. You have to go through requirements gathering, they may and should have a security component to it so that you know what you're looking for in any type of technology to make sure that it meets your standards.

Standards is the other piece of the process. What are your security standards? What kind of information are you looking for? It's funny, I had a customer questionnaire earlier this morning and they wanted me to satisfy their own security needs. I'm a vendor to them. They wanted to understand proprietary and confidential information, which I was unwilling to give. Again, it's about understanding what are the standards, how you satisfy those standards to meet the needs. And then from a requirement standpoint, you fulfill those needs and then you figure out what's the next step of picking the technology if it's cost or you've done business before, but you have to have a whole set of criteria involved in order to pick technology.

I don't know any other way to do it. That's how I've done it through the years. It's tried and proved and I kind of stick with it. The other thing that I would say, from an overall security standpoint, and this isn't just around purchasing new technology, Episerver is a ISO 27,001 shop. If you know anything about the ISO 27,001 standards, it's all around security controls and there are about 133 standards and you have to fulfill a huge chunk of them based on your environment, your company, and what you're doing. Those controls are very explicit around picking, managing, and controlling technology and the controls are everything from accessing technology to making sure that you're setting it up in a controlled, secure environment to monitoring and logging in.

When you put the whole program together, you come away with a very secure program and that secure program is then audited both internally and externally and you identify any gaps and then the next piece of it is continuous improvement. So kind of a long winded answer, but it goes back to purchasing, picking and selecting technology. You just have to have the right considerations in place, the right process, the right standards, and then it shouldn't fail you. And again, it doesn't matter if you're in the office or remote. It should be the same process to move forward to.

**KH**: My last question is around business transformation. Obviously there's a lot going on right now in the current environment that we're in. As businesses continue to transform at a very rapid pace, how can security keep up and keep pace with the business while also focusing on the basic and foundational security principles?

**SB**: I think that right now, in my opinion, it's even more important to make sure that you're keeping pace with what the business is trying to do. There are companies out there fighting for their lives. They've gone from front store to digital or in some cases they haven't. They're trying to get there, to have their own remote business, and security can't be compromised because you're trying to go fast and furious to change your business model to survive. You can be a security minded individual and not impact what's happening out there but lend help to it and make sure that whatever's being delivered from a business perspective is secure. It doesn't have to be a hundred percent the day that it goes out, but at least have a roadmap in place so that you know what has to happen. What's that number one priority if you're going to deliver a new technology or a new business model versus, you know, what's a nice to have versus what can wait. So prioritize based on need and help the business get out there as quickly as possible but don't stand aside and just fold your arms and say it is what it is. That's not the right attitude to have right now in this climate.

**KH**: Well thank you so much Sue, really appreciate all of your insight today and you sharing your advice with our audience here. For our audience, you can learn more about this episode and our other CISO interviews on our website, klogixsecurity.com/podcast.