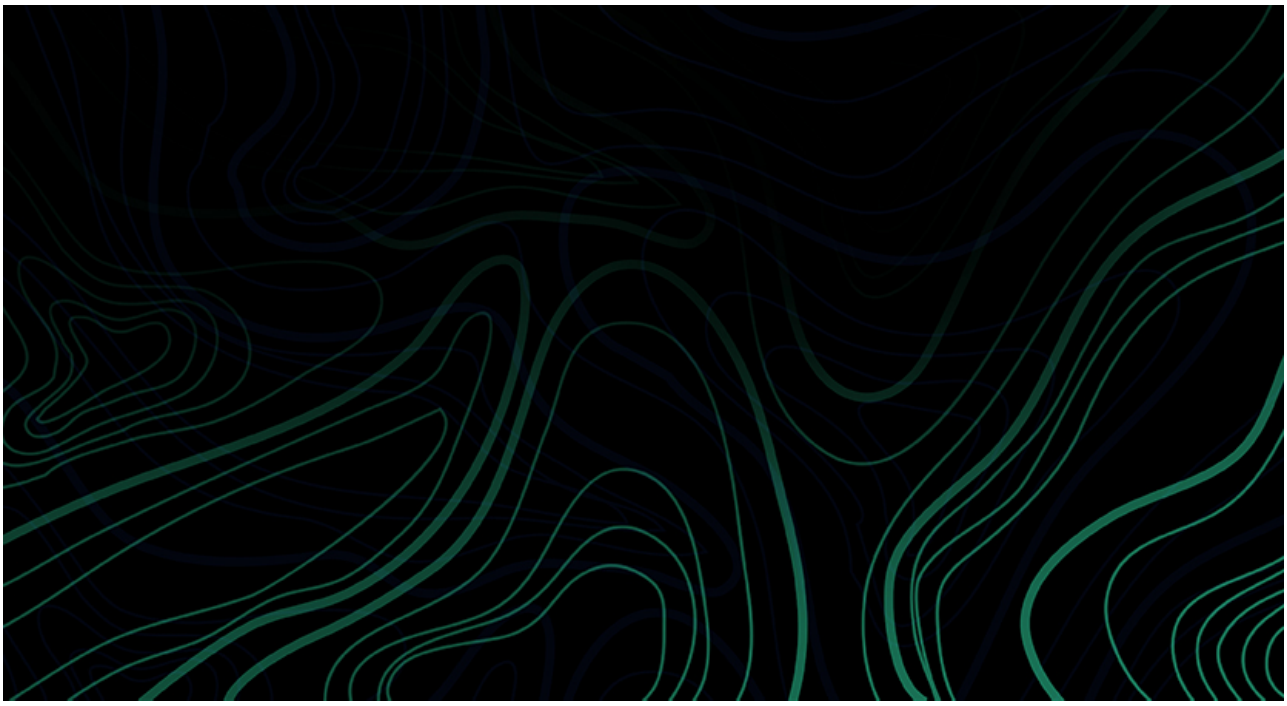
Q&A: Diana Kelley Discusses ROI, Application Security, and Inclusivity

written by Nabil Hannan | July 20, 2021



Cybersecurity leaders hold one of the most difficult positions today, as they're often tasked with protecting an entire organization from sophisticated threats with limited resources. I recently sat down with founding partner and CTO at Security Curve Diana Kelley on the Agent of Influence podcast, a series of interviews with industry leaders and security gurus where we share best practices and trends in the world of cybersecurity and vulnerability management, to discuss key challenges and opportunities security leaders face today. Read on for highlights from our conversation around communicating cybersecurity ROI, building an application security program, inclusivity in the cybersecurity industry, and more.

Nabil: Connecting and conveying a particular message to the C-suite is a common challenge across the security industry. What

has worked well for you when communicating ROI or asking for budget from leadership?

Diana: Cybersecurity ROI can be tough to communicate. First, remember, if you're going to the executives or presenting to the C-suite, you have to look at the world through their lens. We tend to, as technical people, look at it through our lens – which is okay for our understanding, but it is the fiduciary responsibility of the stakeholders of the company to make it profitable. It is important to always think about that, think about how security translates to profitability. Do not go into a leadership or board meeting with technical detail, go in there with "this is what it means" or "this is how it impacts our bottom line."

Second, do not dismiss the fact that their lens is different, as if it is somehow denigrated. The craziest thing I've experienced was a technical person in front of a board of directors say, "I'm the risk expert here." They may have been the technical risk expert, but they didn't understand that the job of the board is risk assessment. It's a different lens of risk assessment, focused on business and profit, but it's still risk.

People always say to speak in the language of business. The way to do this in practice is to remember their lens of profitability, remember that risk is about business risk, and then tie your technical risk in a business way that isn't deeply technical, but is very strong and powerful. You can also share examples, such as, "Did a similar customer lose money due to a competitor having the same problem?" or "Is there new legislation coming down the pipeline that's going to change our implementation and strategy?"

Finally, do not forget to engage leadership in the decision-making process. You want to avoid being demanding, which often happens after a breach or audit. Early on, engage with leadership and communicate the security issues, what it could

mean to your profitability, and explain how the security team can help improve or protect the business in the future. Most importantly, ask if they agree that the investment is a good way to spend the organization's money and ensure you have a consensus.

Nabil: Let's talk about application security. What insight would you give people as they try to decide what frameworks they should use and how to navigate the different options out there?

Diana: Organizations must get an application security program in place – a secure software development lifecycle (SSDLC). This is the most critical part. As far as frameworks go, BSIMM is a good option to understand what other companies that look like you are doing in terms of application security. It allows organizations to have a maturity model to build towards.

Have a framework in place to start implementing an application

security program, create standards for your developers, and start application security testing early on. Identify your application security requirements and understand the threat model so that you can start to build and think about the test harness as soon as possible. It's more important to start implementing rather than focusing on which framework you choose.

It concerns me that now we're getting into this big shift in the enterprise where we're no longer writing code from the ground up, we're doing a lot of low-code no-code. This is fantastic in terms of what we're able to build and how quickly we're able to build it. But companies that are now creating low-code no-code solutions are using a lot of functions and libraries and they are not thinking about it as custom-built code.

I've heard many times, "we don't actually build any applications." Then, you start talking to the company and you find out that they have many scripts that are pulling in functions from the cloud, they're using cool tools like Zappy or Airtable, but they're giving access into parts of their data sets, and they don't realize those scripts are code. I'm hopeful that companies don't solely have an application security program in place, but also an understanding that they need to extend this program to the low-code no-code serverless world that we are moving towards.

Nabil: A lot of the work that you do is focused on inclusivity in the security industry. What advice do you have for security leaders looking for new talent?

Diana: With Women in Cybersecurity (WiCyS) specifically, we're very focused on bringing women into cybersecurity, but there are many different non-profits out there that are looking at cohorts and sectors that have not been involved in cybersecurity in the past. I think security leaders could benefit from getting involved with these organizations to look

for internships for externships.

It’s very common for leaders to say, we can’t find any diverse talent and we had to hire somebody who looks like everybody else because there were no other candidates. Often, it’s not that you didn’t look far enough or hard enough. And that may be because they’re not in your network. If your network doesn’t extend out broadly to different groups of people, then work to expand it.

Be open to people that may not have college degrees, as every job in cybersecurity doesn’t necessarily need a four-year liberal arts degree. Maybe there is somebody who has recently graduated from high school that’s completed the right training. Rethink what you know, how you’re hiring, who you’re hiring, open that aperture wider, and work with those communities that are encouraging inclusivity.

Another tip is to think critically about how you’re writing job descriptions. There is research that shows that women will not apply for a job unless they match about 90% of the criteria or higher, whereas men will apply if they only match 50%. If you write a job description that includes every experience and skill under the sun because you want to get great resumes, what you’re actually doing is turning off the candidates who are reading that job description and believe that, if they don’t have 90 percent or 100 percent of the criteria, they’re not going to be eligible for the job. Rethink your job descriptions: do not gender the job descriptions and make sure that they’re not overstuffed. Write it for what are you looking for and focus on what is important. You’ll be surprised at the resumes it brings in.


AGENT
OF INFLUENCE
EPISODE 030 / Diana Kelley
Communicating Cybersecurity ROI, AppSec Frameworks, AI and ML Security, and More
NETSPI™ Podcast / Hosted by Nabil Hannan
LISTEN NOW