PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JUSTIN BERMAN
CISO, ZENEFITS

HEADQUARTERS: San Francisco, CA

EMPLOYEES: 500

ANNUAL REVENUE: Not disclosed; private company

> "... not only is our company safe, but we're using security to make the company more successful."
>
> **- JUSTIN BERMAN**

Justin Berman re-located from New York to the Bay Area over one year ago to become the new CISO of Zenefits, a provider of cloud-based software-as-a-service for managing human resources, payroll, and benefits. The opportunity and core company mission attracted Berman to make the change and move across the country.

As a leader at Zenefits, Berman embraces the company mission to securely deliver products and services that make it easy for small businesses —the backbone of America's economy—to start, run, grow and thrive.

"We're a payroll, HR, and benefits company," adds Berman. "Therefore, we have a strategic focus and commitment to the kind of controls necessary to protect against both external threats and internal accidents. A testament to that ethos: our executive team determined they needed a CISO with a practical, mature view of risk and security."

He continues, "A bonus to that rigorous approach: not only is our company safe, but we're using security to make the company more successful. The kind of capabilities we want to build here are things that give our customers the confidence that not only are we taking care of their data, we're taking care of them too."

Berman values the commitment Zenefits has to their customers. He says their opportunity is to not just think about being safe enough, but to actually make customers safer by virtue of helping them understand patterns of bad or dangerous behavior. He explains, "People use our tools, and expect we do the job well enough so their data isn't going to get lost. I correlate it to the fact that no one's excited when they turn on their water.

But, they get really upset if their water is off. It's the same thing with security. So, to me, while very important, keeping secure is not enough."

EXECUTIVE ALIGNMENT: LISTEN FIRST, TALK SECOND

When forming and building relationships with executives, Berman believes in listening first and talking second. He says CISOs should come from a place of wanting to help executives do the right thing for the business. By relying on strong listening skills, CISOs should understand the needs of executives, then come up with solutions that move both security and solutions to their challenges forward. This approach resonates with executive advocates and skeptics alike.

For skeptics, Berman's approach is to engage with them more than you would others by pulling them into the decision-making process. He explains, "The skeptics are the ones you should educate by having them be the devil's advocate against your program. They will sharpen your ability to convince other people more effectively. You should actively engage the people that are your biggest doubters and do so consistently. You'll end up converting a meaningful chunk of them over time as they gain more and more confidence in your knowledge and plans through first-hand interaction. If you are sharpening your decisions and your arguments with someone who doubts you, then the people who don't doubt you are going to be convinced very easily."

COMPREHENSIVE APPROACH TO THREATS

"When we talk about insider threat, most people mean the malicious employee. I think it's just as important to consider the employee accident. The latter is a far more likely scenario and worth your focus and time as a CISO, more often than the willfully malicious employee," explains Berman. He says for CISOs who are in the beginning phases of developing insider threat programs, the most important first step is identifying what is most valuable to the organization and which employees have access. Most often, insiders use legitimate access to steal; they typically do not attempt to break systems using complex technological methodologies, according to Berman.

The attention insider threats create is due in part to insiders having so much opportunity, yet Berman does not believe the solution is to create massive monitoring functions for each employee. He continues, "It's about monitoring close to the use or abuse of things that you don't want stolen or manipulated. This is because insiders look very similar to a system that's been compromised by an external adversary. They may be different in the sense that an insider has more awareness of their legitimate access. However, once an insider's device is compromised, that adversary behavior can look very similar. So, really remember the value you're driving from an insider threat program is also protecting against external threats."

"There are going to be a set of threats that you have to plan on defending against, and you can look for the steps within those threat actors' playbooks. Determine if you can defend against the whole playbook by looking at each step and evaluating if you can disrupt it."

Berman believes that planning for and controlling insider threats may vary based on an organization's specific viewpoint and needs. He comments, "Every company has a different view of that problem. It depends on what you're protecting first. What is the value in that? Why would they steal something or what could that do to the company? If they're just trying to steal money, then you're really talking about financial controls, which is a lot different than the security controls you might put in place to prevent data theft."

According to Berman, the biggest risks to any organization are often the adversaries specifically motivated by the organization's business. He says, "There are going to be a set of threats that you have to plan on defending against, and you can look for the steps within those threat actors' playbooks. Determine if you can defend against the whole playbook by looking at each step and evaluating if you can disrupt it. There are just way too many actors with way too many playbooks to laser down which specific threat is the biggest problem. It's not just phishing, it's not just ransomware, it's not just any one thing once you get above a certain scale of organization."