PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JOHAN HYBINETTE

GLOBAL CISO, VONAGE

HEADQUARTERS: Holmdel, New Jersey

EMPLOYEES: 2,000+

ANNUAL REVENUE: $1 Billion

As a well-seasoned security professional, Johan Hybinette has seen first-hand the evolution of the role of security within organizations, transforming from being a historically siloed department into a more business-aligned and impactful program. He says, “What security has become over the years is an interesting perspective. In most companies, you will find that everything’s siloed, yet security talks to every department or every group. Security is basically becoming a collaboration between all departments and actually enabling groups in communication. Where we are today you find many CISOs reporting directly to the board, or working directly for the board or the CEO of the company. And I think that’s proper because the CISO is a conflict of interest virtually anywhere in the company. But the really interesting thing about security is that today security is kind of the glue between the departments of the company.”

Currently the CISO of Vonage, a leading provider of cloud communication services for consumers and businesses, Hybinette joined the organization because of the opportunity to build and enable the security program. He explains, “The most important thing for me, is to roll up your sleeves and get stuff done. I am typically not the CISO in a very mature organization with everything that works and I just keep it running. I’m a builder and an enabler, that’s my trait. I come in, I build it. There has to be budget there, but really what I’m looking for is executive buy-in and board buy-in. If I don’t have buy-in from the top down, I cannot succeed.”

When Hybinette joins a new organization, he ensure he gets himself out within the business to understand everything going on as it relates to business functions and culture. He strongly believes in having an open mind and working hard to fit in with the corporate culture in order to achieve high levels of success.

JOHAN’S PUNCH LIST

Hybinette believes the CISO of today is more of a risk leader than an owner of controls, and someone required to measure risk continuously. He has a formula he’s named “Johan’s Punch List.” He comments, “It’s really a risk register, we meet weekly on the reporting of risk and see how to progress. You

> *“SECURITY IS BASICALLY BECOMING A COLLABORATION BETWEEN ALL DEPARTMENTS AND ACTUALLY ENABLING GROUPS IN COMMUNICATION.”*

get a score between zero and one hundred percent, it gets reported quarterly to the board and the board sees the highest risks. The report is written in a very high-level way so the board can understand what's going on. A lot of security leaders get too technical. It needs to be high-level. In the beginning when you start in a company, there's a lot of doubt from the board and you must report the risk challenges. You want to become agnostic and gain trust in order to become successful."

Hybinette says it is not just the security team who reports on risk, but every department and every division provides their own reports on risk into the main risk register. These risks are then discussed and evaluated with corporate teams, and they determine if the risk is going up, down, or maintained. Timeframes to mitigate risk are also reviewed, creating a comprehensive view into all risks within the organization.

STRATEGIC GOALS AND CHALLENGES

The top strategic goals Hybinette is working towards are putting security into DevOps and going through a transformation program in 2019. He shares, "Cloud is definitely one of the biggest transformation projects. Companies move into the cloud in some way or another, but my thought is that OT is becoming a really large part of security. Everyone thinks about IT security or information technology, but nobody thought of operations technology and how to make all this work. Cloud is basically the first step, and after the cloud, you go through the containers. After container work, you're getting into serverless. So those are several levels of transformation. It's much more complex than that."

Delving further into what transformation means, Hybinette says, "Another huge part of our transformation is access management. Here's an interesting part of that. Access management cannot be owned by the CISO, it has to be owned by IT. Same with CASB. The CISO will not know who's connected to where, when, and why. Only the stakeholders can do that. And that falls into the IT group that generally controls that. Then the CISO organization now reports on the risks of access management. Also, the CISO organization is architecting access management with IT. So maybe doing more of the risk management, architecting the organization, helping the company architect the proper solution and the compliance, and secure it at the same time."

When asked about challenges, Hybinette says people, more specifically training people, is a large priority for him. He says lack of training is often when breaches occur, especially in instances when someone is not doing their job right or something simple occurs such as missing a line of code. He engages in security awareness training and phishing campaigns where he goes into each group and sits down with the team to educate and share his knowledge with them.

When it comes to security awareness training, Hybinette comments, "Most CISOs are very technical but it's the human factor that you really need to focus on. The security awareness tool is only as good as the people operating it. People are training people. You can actually predict what you're getting, and you know the results are going to be there."

CLEARING THE PRODUCT CLUTTER

On addressing the intense clutter of security product companies in the marketspace, Hybinette says many tout the same message as being leaders while using hot industry buzz words to try to sell their solutions.

He comments, "You need to review them and ask what you want that technology to do for you and how it will work in your organization. After you define that, it's basically a process of elimination. You look them all up, you discount the first round. You may want to talk through the second round, and you go through that and demos, then you take off another big chunk of them and you should only have three vendors that basically evaluate against each other. Is this vendor going to survive? I'm so worried about the startups because they want a big name, such as Vonage, under their belt. They want to be acquired. So, everyone's coming after us or companies like our company because of that. We have a very good legal team to make the property contracts."

ADDRESSING PRIVACY LAWS

As a global organization with international offices, Hybinette says when they addressed GDPR they realized 70% is around legal and privacy, not necessarily technical compliance focused. He continues, "That was the lesson learned and that's part of the GRC investments we did, to track GDPR and privacies. Also setting up a whole new policy set, auditing policies, at the same time to ensure GDPR is being followed. It's very difficult to know when you are GDPR ready. What bothers me a lot is that every company says they're GDPR compliant, nobody's fully GDPR compliant. You can only put the GDPR readiness statement on your website, same for California and the other privacy laws.