# PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

## RICK ORLOFF
CISO, ADDEPAR

**HEADQUARTERS:** Mountain View, California

**MEMBERSHIP:** 325

**ASSETS ON PLATFORM:** >$1 Trillion

As an extensively seasoned information security leader, Rick Orloff ensures he delivers actionable results focused on aligning security with real business opportunities that enable the business to achieve goals and objectives. Orloff's notable security leadership positions include leading part of the security program at Apple Inc. around stopping and managing information leaks including protecting Apple's prototype devices and unannounced products and services. His work at Apple Inc. expanded into other security program areas during his 6+ year tenure before moving on as the CISO of eBay where he helped navigate the splitting of eBay and PayPal, among other key initiatives. He then worked as CSO for Code42, a backup and recovery organization, before taking the Chief Security Officer and Chief Privacy Officer position at Addepar, a cloud-based investment management technology startup company.

Among his many accomplishments, Orloff's experience includes business process improvement, structured problem-solving skills, operations leadership, and budget responsibility of $100M. Utilizing process and metrics orientation to build and lead high-performing teams delivering creative world-class solutions, Orloff demonstrates strategic traits including strong analytical, decisive, and technical skills.

## STRENGTHENING CISO AND BOARD ALIGNMENT

In his many years of practice, Orloff experienced the continuing evolution of CISO relationships with their executives and board members. "There needs to be meaningful connective tissue between the CISO and the board. Typically, a CISO has 15 or 20 minutes to run through a deck and provide a snapshot in time. What's also needed is the connective tissue where these CISOs are also talking to one another with the different board companies," says Orloff.

He continues, "Many boards are looking to add security expertise and I'm seeing more CSOs/CISOs being asked to sit on other boards. By including security expertise on the board, there's an opportunity for the board to ask meaningful questions and ensure the company has a reasonable security posture.  Companies that also have security experts participating on their boards seem to embrace security as part of the corporate DNA."

Orloff advises other security leaders to focus board room presentations around a holistic view of what the security program looks like, highlighting core areas of focus. He notes the high value of prioritizing how the program addresses, or mitigates, threats that can affect the "valuation or reputation" of the company. Furthermore, he values the ability to walk board members through how he measures program maturity, progress, and goals.

He states, "At the end of my presentation, I try to educate the board on a couple of items.  Some CISOs conclude a board presentation but the board members may not know what to ask. The question they really need to ask the CSO or CISO is: how do you know if your security program is failing? They just watched a 15 to 20-minute presentation and it looked great, but the CSO/CISO should be prepared to answer difficult questions like this. And if they can't, then it sounds to me like the program is not complete."

When discussing metrics with the board, Orloff believes avoiding generic language, and instead focus on high-level, business impacting specifics. He explains, "The board should be interested in how many critical incidents there were, what the root causes were, and did we fix the root causes. They shouldn't get into vulnerability and patch management or way down in the weeds on the tactics. They should be focusing on the high-level things that are going to indicate the quality of the program."

## THE GROWING THREAT LANDSCAPE AND SPEAR PHISHING

Orloff says traditional security programs were focused on inbound threats and mitigating risks. The approach today has shifted, where teams must figure out what the threats are as categories and put their security programs in place upstream in the data flows or downstream in the technology stack to mitigate those threats. He explains, "One of the biggest threats today is spear phishing. There are different techniques to mitigate phishing attacks that are hitting the servers, but other solutions go further upstream and start to mitigate back at the ISP level. Ideally, we take programs and try to go as far upstream as we can, which gives us more data exhaust to correlate as it's touching our own systems."

According to Orloff, spear phishing presents one of the biggest threats for all verticals. He says since all companies use email, it creates one of the largest threat vectors. With numerous social networks such as LinkedIn, these often are leveraged to craft well-articulated and unique messages to an individual in order to spear phish.

To combat phishing, Orloff relies on best of breed approaches. He says, "The idea is to identify solutions that have the best effective capability, combined with putting a large value on how you measure effectiveness. Don't tell me how many attacks were blocked by the tool, also tell me how many attacks actually made it through. Tell me how and why they made it through."

For Orloff, another critical aspect to combat spear phishing is internal training and awareness. He explains, "When it comes to humans, carbon matters. You've got these spear phishing attacks coming in and now it's all about human behavior and training people to stop, look, and assess that email.  Employees need to question whether or not the email 'attributes' make sense."

"There are anti-phishing training programs out there that are very good. I have seen some corporate programs establish a baseline with a high number of employees getting phished. As that training continues throughout the year, the number of people that were successfully phished dramatically reduces. Results like this validates the importance of an anti-phishing training program."

To stay abreast on the latest threats, Orloff takes a strategic, combination approach. He comments, "It's a combination between reading the newest stuff that's coming out as well as being a member of some key organizations, maybe two or three, so you can speak to your peers to really understand what other people are doing and what risks are manifesting out globally."

### Aligning with Executives Through Strategic Communication

"When aligning with executives, CISOs must focus on their communication style and more specifically, what they are going to communicate. What I have found to be the most successful is not necessarily going in there and talking about problems and how you're going to fix them. What works best is if you start off with talking about the framework by which we're going to operate the department and the problem-solving strategies that we're going to embrace to identify the root problems. A CISO doesn't have to be risk adverse.   What we need to communicate is that we can accept calculated risk, it's important they understand security leadership isn't going to take a position that says I can't accept any risk. There must be a balance to solving important problems, mitigating the less severe problems, and not to be completely shut off to all risk.  There are only three things we can do with risk, i) accept it, ii) transfer it, iii) mitigate it.  It's not possible to eliminate all risks."