# Q&A: EBay's security chief cites evolving cyberthreats

June 16 2015, byMae Anderson

This Feb. 25 2015 photo provided by eBay shows the company's security chief Rick Orloff, at the eBay headquarters in San Jose, Calif. Orloff, 53, a former private investigator, joined eBay Inc. from Apple Inc. last August, just three

months after the company asked 145 million users to change their passwords after a data breach. (Adam Kohler/eBay via AP)

It seems there's nowhere to hide these days from cyberattacks.

Major breaches have exposed critical data at banks, retailers, health care providers and the government, as evidenced by word this month that hackers compromised personal information of at least 4 million current and former federal employees.

Faced with a constant barrage of cyberattacks, its key to stay on top of the latest threats to learn about potential vulnerabilities and effective defenses, says Rick Orloff, the head of security at e-commerce company eBay Inc. Not only must companies protect the traditional layers of security infrastructure, these days it's key to become more sophisticated in detecting attacks and attributing them to the correct source, he said.

And while cybersecurity is critically important for every company, it's particularly so for those that handle consumers' information like eBay, which is responsible for safeguarding sensitive financial information for 25 million sellers and 157 million buyers on its online marketplaces.

The San Jose, California, company has dealt with data breaches before, asking 145 million users to change their passwords following a data breach in the spring of 2014. Orloff, 53, a former private investigator, joined eBay Inc. from Apple Inc. last August, just three months after the breach. He said while that breach has been addressed, the eBay is always looking for ways to improve their security. Since the breach he was worked on creating a war room for the company's security staff and communicating with other companies about cyberthreats.

He spoke with The Associated Press about his top priorities as security chief and the latest thinking on cybersecurity. Below are excerpts of the conversation, edited for length and clarity.

___

Q: How have the recent high profile data breaches affected what you do?

A: What eBay and other companies are doing, we have teams that actually go and inspect other breaches. When we see a company has been breached, we take a look try to understand what was the nature of the breach, what were the strengths, what were the weaknesses, what was the motivation and what was done post-breach. Did (the hackers) just look around or did they take data. One of the reason why this is so important is that this topic and concern for security and customer data is elevated into the C-Level suite and elevated into the boardrooms. People want to understand and are willing to support doing the right thing. It really is key.

Q: Has the media attention been helpful or a hindrance?

A: I think it has been helpful insofar ... . People want to know if they're going to trust a company with their personal information that we're taking the steps necessary to secure it. And they accept that.

Q: What are some lessons learned from studying the Sony breaches and other breaches?

A: On a high level there are primarily three reasons that drive hacker activity. The first one is kind of the category that Sony fell into and that is state-sanctioned or government-authorized hacks. And in that scenario they're usually trying to send a message but it's something that allegedly is authorized by a state or a government. The second category is hackers

that are looking to monetize their hacks. They're out there hoping to get something they can sell and make money. The third one is really your activist hacker. Those are the ones that want to either deface a website to put their message up. They don't do anything really to extract money. They're just trying to send a message, which also falls into your Sony example.

Q: Which one of these types of attacks is the most damaging?

A: The most damaging is really anything that involves customer data or (a company's intellectual property). Hacks being driven by that second example which is to monetize, that's customer data and of the utmost importance to us is to protect that customer data. That is absolute top priority.

Q: How do the different ways to pay like Apple Pay and other digital wallets affect cybersecurity and how can consumers make sure they stay secure?

A: Customers want to pay in the simplest, most convenient way possible. It's actually a great thing. Because it can be tokenization so that customers aren't typing in passwords. I would say that customers, including myself, need to look at their smartphones as their wallets. ... The significant risk to end users and all of our customers is password reuse. As an end user you don't want to reuse the same passwords over and over for all different types of things. Your banking account password should be significantly different than other passwords. The most important password is your email password. Because if a hacker can get into your email account they can go to your bank website and request a password reset. So without even knowing what your bank password is, they can sit in your inbox ask for a password reset from your bank, then they can go to the financial institution and reset the password, and now they have control.

Q: Is there anything that you think people don't understand about cybersecurity?

A: I think that folks don't understand that attacks occur thousands of times an hour and they come from many, many different threat vectors. They can be email attacks, they can be phishing attacks, and I do think that a lot of folks don't understand that one (of the most successful) attacks is through social engineering and phishing and so end-user behavior, just for personal protection, is to be very cautious about what you do with your email and your response to email.

One of the things that really changed in the last year or two is that companies are becoming more collaborative with one another relative to threat information. So there is no exchange of customer data but when it comes to threat information, if we see an attack coming from this entity and this region, companies are sharing that information now as opposed to everyone being siloed.