

It was one of the 17 biggest data breaches of the 21st century: October 2013, hackers stole login information and nearly 3 million credit card numbers from 38 million Adobe users. The company is still dealing with the cleanup, and the recent announcement of a new Experience Cloud feature makes security even more important than before.



Brad Arkin, Adobe CSO

In an exclusive interview with CSO, Adobe CSO Brad Arkin sat down to talk about this past and where security is heading. He was senior director in 2013, the company's highest security title at the time, but Adobe didn't fire him. Instead, Arkin was promoted.

Adobe created a c-level position as one way to improve operations, but Arkin says there was more to it: "There were a bunch of different things happening." Pre-CSO, the director role "focused on the code we were writing for desktop products, which is what Adobe did back then."

Move to cloud creates vulnerabilities

From 2011 to 2013, Adobe shifted from selling desktop licenses to cloud-based, software-as-a-service (SaaS). It was an unavoidable transition for any software company at the time, but also made Adobe vulnerable. "We still had all the desktop code, but we were very much a service delivery company," Arkin explains. "In the old days, the idea [was] that product engineering was totally separate from IT security [and that] didn't really hold anymore."

Over two years, Arkin found himself managing security “not just [for] the code that we write, but the servers and the infrastructure that it runs on and...things that you see [as] traditional back-office stuff, things like IT security” — without any c-level authority.

A part of what it means to be secure is that people have to feel secure. — *Brad Arkin*

Naming a CSO went a long way toward creating a sense of security theater, something Arkin has to constantly think about. One lesson his team learned in 2013 is that “doing a good job for security is only part of it. A part of what it means to be secure is that people have to feel secure.”

Arkin set out to improve security privately, but to communicate publicly. In addition to creating the CSO role, Adobe underwent a broader reorg, he says, “working to integrate all the different pockets of security teams,” clarifying priorities, and uncovering “organizational blind spots.” Having a CSO gave staff a clearly defined leader to point to. Communicating the position’s creation improved optics. “By creating the CSO role, we were making it really clear internally that I’m on the hook to figure this stuff out,” he explains.

The least bad option is always transparent communication. — *Brad Arkin*

By on the hook, Arkin means that if there is another breach, his face will be front and center. “We put a big emphasis on transparent communication,” he says. “If something bad happens, your first reaction would be, ‘Oh, I wish this didn’t happen, I’m embarrassed, I’m upset,’ and the temptation [is] to not talk about it. That is rarely the right strategy. The least bad option is always transparent communication.”

Yes, Adobe underwent a \$1 million breach. Yes, 15 different states sued them for it. But Arkin and his team own it. They’ve taken steps to prevent another one from happening. Should those steps fail, Adobe promises to let us know.

Adobe Experience Cloud's security challenge

They'd better make good on that promise to let us know. In his March 27 keynote at Adobe Summit — the company's annual user event — executive vice-president of digital marketing Brad Rencher bragged about Adobe Experience Cloud's newest feature: a unified profile that centralizes every data point an Adobe customer has ever collected about you.

Rencher calls it "a new system of record, one that can manage and make sense of the high volume of content and data." The unified profile collects individual browsing behavior, device use data, customer relationship management (CRM) notations, information from Microsoft Dynamics 365, and more. The goal is to make personalized marketing, well, more personalized. From a security standpoint, the unified profile theoretically has the hacking potential of personally identifiable information (PII) in a to-go bag.

Talk about tough security theater.

It isn't Arkin's job to design features, rather to protect them. "In our experience, it doesn't matter as much how secure a code base is. It's all about what the install base looks like and how attractive is it to the adversary," he says.

In our experience, it doesn't matter as much how secure a code base is. It's all about what the install base looks like and how attractive is it to the adversary. — *Brad Arkin*

Another 2013 lesson learned, he continues, "is that it's very much about who the potential adversaries are and what are their objectives." The more machines or data a hacker can access, the higher risk to the target. That's why Adobe has traditionally focused heavily on protecting Flash Player, which Arkin says is installed on billions of systems.

While Experience Cloud has fewer users, the companies that buy it collect data on millions of their own customers. "Getting a remote code execution on the target's machine is usually a starting-point objective for the bad guy to then help them achieve whatever the outcome is," Arkin says. What he sees "happening more and more is that bad guys are looking more to steal

credentials than they are to run untrusted code...because it's really hard to get the code onto the machine now, compared to what you could do to a Windows machine 10 years ago."

Authorization key to cloud security

To protect Experience Cloud — or any other cloud-based program — authorization is critical. Arkin says, "Someone with the user ID and password might be accessing the account, but if they're behaving in a way that's different, maybe it's not actually the true owner. It might be a different human using those credentials. So, how can we better understand what normal is for particular accounts and then identify anomalies, and then what's the right way to react to that?"

For basics like "a yes/no decision based on the characteristics of the login attempt," Arkin says Adobe works with Okta, explaining the vendor's "one component inside of a bigger architecture." With zero trust and internal authorization builds, he says, "We're able to reach in and ask more detailed questions about the device that we're talking to. Does it have the certificates installed that we pushed there when we first configured the machine? Is it running our mobile device management software? What's the patch level?"

According to Arkin, authorization is so thorough, Adobe sales staff have gotten locked out at conferences: "We had an Adobe employee who always used iPhone and Mac from the Seattle office. All of a sudden, we saw his account being used to log in from five different Windows machines in Las Vegas within 20 minutes and we were like, 'Oh, we got a hot one!'...That was a really fun situation," Arkin jokes.

When you've been through a breach so bad that reporters still ask about it nearly five years later, sales staff will just have to deal with situations like that. Like any other company, Adobe security still isn't perfect: Minor issues surface, like that PGP encryption key posted on the company blog last September, but since 2013, the company's seen nothing on a massive scale.

That proactive work that we do through defense in depth, that's great, but you've got to be prepared to react and respond when something doesn't go right. — *Brad Arkin*

When asked if minor leaks can't add up to major problems, Arkin stresses the need to "proactively make things secure through a strategy of defense in depth," explaining that doesn't mean putting "one line of defense in place and then say[ing], 'Oh, let's just write perfect code and then we'll be safe.'" Because we know that code can have flaws and so you need to have multiple layers of defense. That proactive work that we do through defense in depth, that's great, but you've got to be prepared to react and respond when something doesn't go right."