DATA BREACH DEBRIEF

UNDER ARMOUR'S response to a cyber attack achieved the seemingly impossible: Rather than fueling outrage, it actually drew praise. Brunswick's **SIOBHAN GORMAN** reports.

In late March last year, Under Armour learned that its MyFitnessPal app, which tracks diet and exercise, had a data breach that affected 150 million users. It's not uncommon for companies to take several weeks—or even months—to publicly announce a cyber attack of that scale.

Under Armour did so in four days.

Observers praised the speed of Under Armour's response and the concern it showed for users, whom the company also refers to as athletes. A Forbes article published one day after the company announced the attack said, "Kudos to Under Armour for its response so far." Roughly a month after the announcement, Under Armour's share price was up more than 9 percent; after announcing a data breach that affected 143 million consumers, Equifax's share price had sunk by more than 11 percent a month later.

Brunswick's Siobhan Gorman, who advised Under Armour, revisits the event with the three women who led the company's response:

C.M. Tokë Vandervoort, Senior Vice President at Under Armour and Deputy General Counsel at the time of the breach.

Kelley McCormick, Senior Vice President at Under Armour, Corporate Communications.

Lisa Sotto, Chair of Hunton Andrews Kurth's global privacy and cybersecurity practice, and Managing Partner of the law firm's New York office, who was brought in as outside legal counsel.

In their re-telling, the team was able to act with such speed because they had built a level of trust seldom found in a large, global company. And the strategy was dictated by something almost every company has but often loses sight of during a crisis: core values.

TOKË VANDERVOORT: March 23rd was a Friday, and that night and the following afternoon we received two separate tips. One of our guys heard through a back-channel whisper on LinkedIn, "I've got some information that might be interesting to you." It was just a sample of dated data—not enough to do anything with. The next day we got word that it looked like there was more, but we didn't have more information than that.

Then on Sunday, an undisclosed but trusted source said they had a file for us. After four hours of trying to download this file—it wasn't timing out, it was still downloading—I realized we had a problem. When we were able to start accessing that file, we realized very quickly what the situation was. That was about 8 on Sunday night. As leads for the incident response team—one of my many roles as Deputy General Counsel—our information security officer and I called it a breach that night.

My first call on Monday [March 26th] morning was to John Stanton, [EVP and General Counsel at Under Armour]. I remember it vividly because his question was, "Why are you calling me before 8 on a Monday? It can't be good." And I said, "It's not."

Then I called Lisa as outside legal counsel. The relationship with Lisa was one that was already established by Under Armour, but I also knew her well as the go-to professional in this space.

We notified key people, like Paul Fipps, our Chief Digital Officer, and soon after we created a war-room: papered the windows, opened up a phone line, started keeping notes on a white board in terms of a timeline, people, contacts, contractors, things like that. Records on the wall were literally being made in real time.

Our team was also working with outside forensics teams to make sure nothing else was going on. We were trying to ascertain the problem, fix the problem and find any other breakages along the way—all at the same time.

And then the news went to the executive leadership team that morning.

KELLEY McCORMICK: I'd only been with the brand for about three months, and that was my second ex-

ILLUSTRATION: HANNA BARCZYK

ecutive leadership team meeting. I was learning a lot about the ethos of the company and how the brand was built. I was still figuring out functions of teams.

After finding out, it wasn't who to call, it was what part of the company was I calling? I had the luxury of having people—both our team in-house and outside advisers—to help us think through the process. And I was literally learning about the company and discovering our amazing capabilities in the process.

TV: I remember Kelley being in John's office and saying very humbly, "This is where my job gets easy because I do what legal tells me." I knew your job wasn't going to be easy at all, but it was funny.

KM: There are times when communications can challenge legal to relax or be more aggressive. But given the nature of this situation, I felt the default had to go to legal. I wanted to diminish that debate.

TV: After he had processed the news, Paul Fipps, our Chief Digital Officer, pulled the team together. His first inclination was essentially: "We recently relaunched our core values and those will inform how we do this." Guided by those values, he wanted us to go public with the information before markets closed on Thursday. Because Friday was Good Friday, a market holiday. And then you have the weekend. Nobody wants to go out on a Friday. It's considered crummy. The holiday sort of threw us into that aggressive push to get it out by Thursday.

> "We recently relaunched our core values and those will inform how we do this."
>
> The direction **PAUL FIPPS**, Under Armour's Chief Digital Officer, gave to his team.

But, of course, the last thing you want is to go out twice. You look incompetent, right? So it not only had to be very fast, it had to be right. I remember a conversation where we were asked, "Can you do it by Thursday?" And I said, "We're going to try." And the response was: "That wasn't my question."

KM: We didn't want our athletes to wake up the following Monday and have them say, "You knew about this for eight days and didn't say anything?" We wanted to make sure they had the information so that they could decide what they were going to do about it.

With those values as a kind of compass, a number of decisions were strangely easy to make. The guardrails were really: What was the right thing for athletes, what were our values? Almost everybody's got a value statement these days. It was cool when you put it in context of a digital event, not just shirts and shoes.

TV: From a legal perspective, the average timeframe from knowing to disclosing is somewhere around 30

days, give or take. We could have done that. This information wasn't passport numbers and Social Security numbers. It was their name, their user name, their email address and a couple of other data points that would be unlikely to lead to financial fraud. But the idea of that information being used for phishing, to trick people and make them feel vulnerable, was very real. The notion of how much time you have under a reasonableness test is one thing, but coming out ahead of time so that people can protect themselves quickly is important.

We had one huge file, and it was the entire file. We knew there wasn't anything else because our system doesn't store credit card information. Even though we take credit card information for a premium subscription, it was, by design, a completely separate data stream. That information was never stored in that file—it wasn't even stored in our systems and we assured ourselves that no connection could have been made between our event and those third-party credit card processors.

LISA SOTTO: We were able to gain confidence about containment of the breach quickly thanks to the technical folks who were working on this incident. It was clear early on that we knew what had happened and based on that clear knowledge, there was no need to wait.

Now, is there the possibility that we might have discovered other files? In some sense you're taking that risk. But we had a high degree of confidence because of the way the systems were designed and the nature of the incident.

We worked around the clock to get the communications in order for both affected users and also to relevant regulators. We also readied talking points for a call to regulators so that everything would be consistent.

It's important to note that this was not an incident that would trigger notification in a number of jurisdictions, including the United States. There were some notification obligations that were triggered overseas, but not in the United States. Many companies would have avoided global notification in favor of a pinpointed approach. But Under Armour did not look to parse jurisdictions and legal requirements.

So we wanted to make sure that all users got the same message regardless of what the actual legal requirements were. Under Armour went far above and beyond its legal obligations.

My firm represents a lot of Fortune 500 companies; these are very compliance-oriented businesses, deeply protective of their reputations and their brands. So it's not uncommon for them, in a response to a crisis situation, to put the user or the customer first. But what is uncommon is an absolutely explicit focus, the mandate by senior leadership, to require that every action be taken through that lens of core values and what's best for the user.

"Almost everybody's got a value statement these days. It was cool when you put it in context of a digital event, not just shirts and shoes."

KELLEY McCORMICK
Under Armour's Senior Vice President, Corporate Communications.

"You know it's going to make headlines. The number's too big not to. Doing the right thing was more important than doing the required thing."

TOKË VANDERVOORT
Senior Vice President at Under Armour.

TV: I don't know that it ever even legitimately occurred to us to parse the communications; we knew we had a huge number of users globally and that a lack of consistency in the messaging would have just gotten us completely shredded.

Creating something that was sort of all things to all people, under all paradigms, was an interesting drafting exercise, to be sure. But again, the combination of our values and the risk of not taking that approach reputationally I don't recall ever even being a serious alternative.

It's one of those things where you know it's going to make headlines. The number's too big not to. Doing the right thing was more important than doing the required thing. In a perfect world, those would be the same, but they're not. The highest common denominator was the right approach.

So you fast-forward to Tuesday afternoon, and there was a growing consensus that Kevin [Plank, founder, CEO and Chairman of Under Armour] needed to be brought in and informed. We agreed that John Stanton, the most even-keeled general counsel on the planet, should tell him.

As John tells it, he delivered the news to Kevin. I asked how Kevin had taken the news, and John said, "Well, when the color came back to his face, he had some great questions and asked for a full briefing tomorrow."

The pace continued from there. There wasn't much sleep.

The next day, we gave Kevin the nuts-and-bolts briefing. He had a lot of questions; some we had the answers to, some we were still in flight with.

KM: Our communications to users—we prepared to blanket them. We created email communications to go out to all of those email addresses. We readied in-app notifications, banner notifications, and push notifications. On the website as well. We even prepared something on the UA.com homepage so people could be redirected to that.

There were also communications prepared for our major sponsored athletes, in case they received any questions about the attack, so that they knew where to refer those questions.

LS: This involved an enormous number of users who needed to be contacted. All of the different paths toward communication were so critical, and with each, we needed to take a global approach. We had to be both legally and culturally sensitive, using a highest common denominator global approach—for each message. That was the crazy part. I remember drafting each message that would go out globally, spending time on the nuances of each, so that we were always consistent. It was a lot of work, a lot of coordination.

TV: We had to translate materials. We had an internal leadership communication and an internal teammate communication that were going to go out just before the public communication as well—Under Armour has 14,000 people globally. It was an astonishing array; the checklist of communications was really quite breathtaking and comprehensive.

And there were obviously detailed FAQs that were being prepared, while key concepts were being programmed into our AI system used by "Customer Happiness"—Under Armour's team of amazing customer support professionals who answer questions about our apps and handle customer care.

That team was an ace up our sleeve because not everybody has that in-house capability. Customer Happiness helped inform our response and keep it user-focused—they were given a direct line into that war room. They were just amazing in handling all of the questions that came in. We were piping in food and water to them, sending them massage therapists for weeks afterwards, because they would deal with an unbelievable volume of inquiries over the next several weeks.

But before that all went live, one of the things that Kelley and I had to do on Thursday afternoon was brief Kevin on those internal and external communications. He was traveling to New York so Kelley and I rode with him in a car. Kevin's up front and Kelley's reading the statements and as questions come up, we're fielding them.

The car stops and a helicopter's waiting in the distance. Kevin gets out of the truck and slings his backpack over his shoulder and puts his sunglasses on. Then he gives us a thumbs-up and says, "Go," before turning around and getting on a helicopter.

And Kelley and I are standing there, thunderstruck by what just happened. We look at each other, and we're just watching the helicopter take off, and I said, "I think we're a go."

And at 4:31 that afternoon, we went. ◆

ILLUSTRATION: HANNA BARCZYK

"We wanted to make sure that all users got the same message regardless of what the actual legal requirements were. Under Armour went far above and beyond its legal obligations."

LISA SOTTO
Chair of Hunton Andrews Kurth's global privacy and cybersecurity practice.

SIOBHAN GORMAN is a Partner in Brunswick's Washington, DC office. A specialist in crisis and cybersecurity, she advised Under Armour on its response.

WHAT MADE THE DIFFERENCE

As told by Tokë Vandervoort

1. RELATIONSHIPS
External relationships are how we found out about the breach, and they're how we knew which advisers and expertise to bring on board right away. We had those in place and had put a lot of effort into maintaining them and keeping them up to date. Internally, the trust we'd built allowed us to move as quickly as we did. Both paid huge dividends.

2. PREPAREDNESS
I don't know anybody whose incident response team meets every other week, but ours does. Sometimes we're just shooting the breeze, but other times we're asking: "What's going on in the business? What are you hearing? What's happening?" We enjoy a great relationship with the product team, the engineering team, the IT security team, the IT team ... It's not just sharing information, but also getting to know one another, which ties back to the importance of relationships—knowing what's going on and who to call.

3. PRACTICE
We do a table top every year for a data incident. I've heard people say table tops are too expensive—we make up our own. Security and privacy get together and create a two- or three-hour game. One year it'll be a supply chain issue, another year it'll be a data event.

We invite decision-makers from across the organization so that people then have a sense of what it feels like to make decisions without full information and to have to do so under a lot of pressure.

People appreciate not just how hard these decisions are, but they know who the other people are, and the issues that they're confronted with. The companies that have the most confident response are the ones where everybody knows their roles—not some giant team of people who have never worked together. When you have complete clarity of purpose, focus and leadership, you can get anything done.