

Opening Statement of

Tim Schaaff

President of Sony Network Entertainment International

Before the Subcommittee on Commerce, Manufacturing and Trade
of the U.S. House of Representatives Committee on Energy and Commerce

Washington, DC

June 2, 2011

Chairman Bono Mack, Ranking Member Butterfield, and other distinguished members of the Subcommittee, thank you for providing Sony with this opportunity to testify on cyber crime and data security.

My name is Tim Schaaff, and I am President of Sony Network Entertainment International, a subsidiary of Sony Corporation based in California, where we employ approximately 700 people in five offices around the state.

I am chiefly responsible for the business and technical aspects of Sony's PlayStation Network and Qriocity, online services that allow consumers to access movies, television shows, music and video games.

Sony Network Entertainment, Sony Online Entertainment and millions of our customers were recently the victims of an increasingly common digital-age crime: a cyber attack.

Indeed, we have been reminded in recent days of the fact that no one is immune from the threat of cyber attack; businesses, government entities, public institutions and individuals can all become victims.

We applaud the Subcommittee and your colleagues in Congress for your work on cyber security, and we look forward to working with you to make the Internet a safer place for everyone to learn, enjoy entertainment and engage in commerce.

The attack on us was, we believe, unprecedented in its size and scope. Initially, Anonymous, the underground group associated with last year's WikiLeaks-related cyber attacks, openly called for and carried out massive "denial-of-service" attacks against numerous Sony Internet sites in retaliation for Sony bringing an action in federal court to protect its intellectual property. During or shortly after those attacks, one or more highly skilled hackers infiltrated the servers of the PlayStation Network and Sony Online Entertainment.

Sony Network Entertainment and Sony Online Entertainment have always made concerted and substantial efforts to maintain and improve their data security systems. We hired a well-respected and experienced cyber-security firm to enhance our defenses against the denial-of-service attacks threatened by Anonymous. But unfortunately no entity – be it a mom-and-pop business, a multinational corporation, or the federal government – can foresee every potential cyber-security threat.

On Tuesday, April 19, 2011, our network team discovered unplanned and unusual activity taking place on four of the many servers that comprise the PlayStation Network. The network team took those four servers off line and an internal assessment began.

On Wednesday, April 20th, we mobilized a larger internal team to assist in the investigation. And on that date, the team discovered the first credible indications that an intruder had been attempting to access customer data in the PlayStation Network system. We immediately shut down all of the PlayStation Network services in order to prevent additional unauthorized activity.

That same afternoon, we retained a security firm to “mirror” the servers to enable a forensic analysis. The scope and complexity of the investigation grew substantially as additional evidence about the attack developed.

On Thursday, April 21st, a second recognized firm was retained to assist in the investigation.

On Friday, April 22nd, we notified PlayStation Network customers via a post on the PlayStation Blog that an intrusion had occurred. That blog, by the way, has been rated one of the top-twenty most influential on the Internet, right behind the White House’s blog. It has a highly visible and deeply engaging relationship with our customers and is one of the best, fastest and most direct means of communicating with them.

By the evening of Saturday, April 23rd, we were able to confirm that intruders had used very sophisticated and aggressive techniques to obtain unauthorized access to the servers and hide their presence from the system administrators.

On Sunday, April 24th, yet another forensic team with highly specialized skills was retained to help determine the scope of the intrusion.

By Monday, April 25th, we were able to confirm the scope of the personal data that we believed had been accessed. Although there was no evidence credit card information was accessed, we could not rule out the possibility:

The very next day - Tuesday, April 26th - we issued a public notice that we believed the personal information of our customers had been taken and that, while there was no evidence that credit card data was taken, we could not rule out the possibility. We also posted this on our blog and began to email each of our account-holders directly.

On Sunday, May 1st, Sony Online Entertainment, a multiplayer, online video game network, discovered that data may have been taken. On Monday, May 2nd, Sony Online

Entertainment shut down this service and notified customers that their personal information may have been compromised.

Throughout this time, we felt a keen sense of responsibility to our customers:

- We shut down the networks to protect against further unauthorized activity.
- We notified our customers promptly when we had specific, accurate and useful information.
- We thanked our customers for their patience and loyalty and addressed their concerns arising from this breach with identity theft protection programs for US and other customers (where available) and a “Welcome Back” package of extended and free subscriptions, games and other services.
- And we worked to restore our networks with stronger security to protect our customers’ interests.

Let me address the specific issue you are considering today – notification of consumers when data breaches occur. Laws – and common sense – provide for companies to investigate breaches, gather the facts, and then report data losses publicly. If you reverse that order – issuing vague or speculative statements before you have specific and reliable information – you either confuse and panic people, without giving them useful facts, or you bombard them with so many announcements that they become background noise.

As recently noted by Director of National Intelligence James Clapper, “...almost two-thirds of US firms report that they have been the victim of cyber security incidents or information breaches.” So we must strike the right balance between giving people the information they need, when they need it, without sounding false alarms or so many alarms that these warnings are ignored.

We support federal data breach legislation that would: (1) provide consumers the assurance that if and when their personal data is compromised, they will receive timely, meaningful and accurate notice of this fact; (2) ensure that consumers receive helpful information on what measures they can take to mitigate any potential harm; and (3) provide uniformity so consumers are treated equally no matter what state they live in and businesses no longer have to navigate varying and sometimes seemingly conflicting state laws in this field.

One final point: as frustrating as the loss of networks for playing games was for our customers, the consequences of cyber attacks against financial or defense institutions can be devastating for our economy and security. Consider the fact that defense contractor Lockheed Martin and the Oak Ridge National Laboratory, which helps the Department of Energy secure the nation’s electric grid, were cyber attacked within the past two months.

By working together to enact meaningful cyber-security legislation, we can limit the threat posed to us all. We look forward to this initiative to ensure that consumers are empowered with the information and tools they need to protect themselves from cyber criminals.

As the Subcommittee is aware, we have submitted letters responding to a variety of questions posed by the Subcommittee regarding the details of the cyber attack we experienced, and I ask that those letters be submitted as part of the record of this hearing.

Thank you.