Sony: The World's Largest Data Breach?

CASE STUDY

On April 19, 2011, system administrators at Sony's online gaming service PlayStation Network (PSN), with over 77 million users, began to notice suspicious activity on some of its 130 servers spread across the globe. The PlayStation Network is used by Sony game machine owners to play against one another, chat online, and watch video streamed over the Internet. The largest single data breach in Internet history was taking place.

On April 20, Sony engineers discovered that some data had likely been transferred from its servers to outside computers. The nature of the data transferred was not yet known but it could have included credit card and personal information of PlayStation customers. Because of the uncertainty of the data loss, Sony shut down its entire global PlayStation network when it realized it no longer controlled the personal information contained on these servers.

On April 22, Sony informed the FBI of the potential massive data leakage. On April 26, Sony notified the 40 states that have legislation requiring corporations to announce their data breaches (there is no similar federal law at this time), and made a public announcement that hackers had stolen some personal information from all 77 million users, and possibly credit card information from 12 million users. Sony did not know exactly what personal information had been stolen.

The hackers corrupted Sony's servers, causing them to mysteriously reboot. The rogue program deleted all log files to hide its operation. Once inside Sony's servers, the rogue software transferred personal and credit card information on millions of PlayStation users. On May 2, Sony shut down a second service, Sony Online Entertainment, a San Diego-based subsidiary that makes multiplayer games for personal computers. Sony believed hackers had transferred personal customer information such as names, birth dates, and addresses from these servers as well. This was not the result of a second attack but rather part of the earlier attack not immediately discovered. On June 1, Sony Pictures Entertainment's Web site was also hacked, and drained of personal information on its several million customers, in addition to 75,000 "music codes" and 3.5 million coupons.

The total Sony data breach now numbers over 100 million customers. In a normal year, the reported total losses of personal information from online systems in the United States involves about 100 million people. Sony exceeded this in a single attack.

The Sony data breach was apparently the result of a "revenge hacking," the use of the Internet to destroy or disrupt political opponents, or to punish organizations for their public behavior. Currently, it is not clear that any credit card information has actually been abused by hackers. According to Sony, hackers left a text file named Anonymous on Sony's server with the words "We are legion." Anonymous is the name of an Internet collective of hackers and vigilantes whose motto is "We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us." Anonymous in December 2010 had attacked MasterCard and other company servers in retaliation for cutting their financial relationships with WikiLeaks, a Web site devoted to releasing secret American government files.

Sony and others believe the hacker attack, which followed weeks of a denial-of-service attack on the same Sony servers, was retaliation by Anonymous for Sony's civil suit against George Hotz, one of the world's best known hackers. Hotz cracked the iPhone operating system in 2008, and in 2010 cracked the Sony PlayStation client operating system and later published the procedures on his Web site. Anonymous denied that as an organization it stole credit cards, but the statement is unclear about whether its members as individuals participated in the attack. Anonymous claims Sony is simply trying to discredit Anonymous instead of admitting its own incompetence in computer security.

Sony's Board Chairman apologized to its users and critics in the United States Congress for the security breakdown. Nevertheless, governments around the world reacted harshly to the lapse in security at Sony. The U.S. House Committee on Commerce, Manufacturing, and Trading criticized Sony for not knowing what data had been transferred and for failing to inform customers immediately rather than waiting a week before going public. In a letter to Sony Board Chairman Kazuo Hirai, the committee demanded specifics on the kind of information the hackers stole and assurances that no credit card data were swiped.

Representative Edward J. Markey (D-Mass.) said hackers and thieves shouldn't be playing "Grand Theft Auto" with millions of addresses, emails and other sensitive information. In a letter of apology to the Committee and Sony customers, Chairman Hirai said Sony has been the victim of a very carefully planned, very professional, highly sophisticated criminal cyber attack designed to steal personal and credit card information for illegal purposes.

This is the "Darth Vader" defense that many organizations use when they experience a gross breach of security: whatever it was, they believe it was extremely sophisticated, totally unprecedented, and could not possibly have been anticipated.

Many experts in computer security did not buy Sony's explanation. In fact, most computer security breaches are the result of fairly simple tactics, management failure to anticipate well-known security risks, unwillingness to spend resources on expensive security measures, sloppy procedures, lack of training, carelessness, and outdated software. Many hacking attacks use simple, well-known approaches that seem obvious. The hack of Google's computers in late 2010 resulted from a single employee responding to a phishing e-mail from what he thought was Google's human resources department.

Appearing before the House Energy and Commerce Committee, Eugene Spafford, the executive director of the Purdue University Center for Education and Research in Information Assurance and Security (CERIAS), said the problem at Sony was that the PlayStation Network was using an older version of Apache Web server software, which has well-known security issues. In addition, Sony's Web site had very poor firewall protection. He said the problem was reported on an open forum months before the incident. A U.S. Secret Service agent told the committee that the vast majority of attacks on databases were not highly difficult. Moreover, once hackers are on the inside, critical personal information and credit information are usually not encrypted. If such information were encrypted, hackers would not be able to read the data. The reason most personal data are not encrypted in large-scale private databases is cost, and to a lesser extent speed. Data encryption of the sort needed for an operation like Sony's could easily require a doubling of computing capacity at Sony. This would significantly eat into profits for an Internet-based enterprise like Sony simply because IT is such a huge part of its cost structure.

A group calling itself LulzSec claimed responsibility for the later attack on Sony Pictures. Rather than announcing new powerful methods of hacking sites, the group claimed Sony's lax security allowed it to perform a standard SQL injection attack on a primitive security hole that enabled it to access whatever information it wanted.

Sony notified its customers of the data breach by posting a press release on its blog. It did not e-mail customers. Since the data breach, Sony has offered customers free games and privacy protection ("AllClear ID Plus") offered by a private security firm at Sony's expense for customers concerned about protecting their online identity. This offer is distributed to user e-mail accounts. The privacy protection plan does not offer an insurance policy against potential losses, but does help individuals monitor the use of their personal information by others. The company anticipated that it would have to pay $170 million in the 2011 financial year for these measures, plus associated legal costs.

It took Sony four weeks to restore partial PlayStation service, and by May 31, the company had restored service to the United Sates, Europe, and Asia except for Japan. So far, no law enforcement agency has reported illegal use of credit cards stolen in the Sony affair.

According to Frank Kenney, vice president of global security at Ipswitch, a company specializing in transferring files securely online, the fact that dozens of Sony Web sites and servers had been breached is a sure sign of a company-wide problem. Any type of environment can be breached, but Sony has to devise a plan that not only protects its infrastructure but also convinces customers that their credit card and personal information are safe. Sony's brand is at stake, he said. Sony's security problems could take years to fix.

The Sony data breach follows a string of recent breaches that are larger and broader in scope than ever before. The Privacy Rights Clearinghouse keeps a database of known data breaches. Prior to the Sony debacle, the largest data breach in 2011 occurred at Epsilon, the world's largest permission-based e-mail marketing services company with more than 2,500 corporate customers, including many major banks and brokerage firms, TiVo, Walgreens, and major universities. Epsilon sends out 40 billion e-mail messages a year for its clients. In April 2011, Epsilon announced a security breach in which millions of e-mail addresses were transferred to outside servers. One result of this breach was millions of phishing

e-mails to customers and the potential for the loss of financial assets.

As data breaches rise in significance and frequency, the Obama administration and Congress have proposed new legislation that would require firms to report data breaches within specific time frames, and sets standards for data security. The Data Accountability and Trust Act of 2011 being considered by Congress requires firms to establish security requirements and policies, notify potential victims of a data loss "without unreasonable delay," and notify a major media outlet and all major credit reporting agencies within 60 days if the credit card data on more than 5,000 individuals are at risk. Currently, 46 states have such legislation. In the past, many organizations failed to report data breaches for fear of harming their brand images. It is unclear if the proposed legislation would reduce the incidence of data breaches.

Sources: "Cody Kretsinger, Accused LulzSec Hacker, Pleads Guilty in Sony Hacking Case," Reuters, April 5, 2012; Riva Richmond, "Hacker Group Claims Responsibility for New Sony Break-In," *The New York Times*, June 2, 2011; Ian Sherr and Amy Schatz, "Sony Details Hacker Attack," *The Wall Street Journal*, May 5, 2011; Jesse Emspak, "Expert: Sony Had Outdated Software, Lax Security," IBtimes.com, May 5, 2011; Eugene Spafford," Testimony before the House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade, Hearing on "The Threat of Data Theft to American Consumers" May 5, 2011; "Data Accountability and Trust Act" 112th Congress, H.R. 1707, May 4, 2011; Martyn Williams, "PlayStation Network Hack Will Cost Sony $170M," PC World, May 23, 2011; Nick Bilton, "Sony's Security Problems Could Take Years to Fix," *The New York Times*, June 6, 2011; "Letter to Honorable Mary Bono Black and Ranking Member Butterfield, Sub Committee on Commerce, Manufacturing, and Trade, United States Congress," by Kazuo Jirai, Chairman of the Board, Sony Corporation, May 3, 2011; Ian Sherr "Hackers Breach Second Sony Service," *The Wall Street Journal*, May 2, 2011; "International Strategy for Cyberspace," Office of the President, May 2011; "Epsilon Notifies Clients of Unauthorized Entry into Email System," Press Release, Epsilon Corporation, April 1, 2011.

CASE STUDY QUESTIONS

1. List and describe the security and control weaknesses at Sony that are discussed in this case.
2. What management, organizational, and technology factors contributed to these problems?
3. What was the business impact of the Sony data losses on Sony and its customers?
4. What solutions would you suggest to prevent these problems?