2011 SONY PLAYSTATION NETWORK BREACH

Short Research Paper #1

SEPTEMBER 3, 2023

CYSE 300

BRYANT WATKINS

Shortly after the first quarter of the year 2011, Sony and its PlayStation Network began experiencing technical issues that prevented users from across the world from being able to access it. At the time and still holding true today – Sony PlayStation Network experienced one of the largest data breaches and external intrusions ever seen. Shortly after experiencing issues with the network, it began to be reported that user information for as many as 77 million people had been compromised. This breach would send waves throughout the cybersecurity world and forever change the way we think of and execute cybersecurity.

There was a plethora of vulnerabilities that contributed directly to this data breach of Sony PlayStation Network user information. Some of these vulnerabilities include – insufficient employee safety training/education, lack of data encryption, and an inadequate alarm/response system. Many critics and experts have repeatedly pointed out that many of these vulnerabilities were preventable. A later revealed set of emails from within Sony publicized the fact that Sony had long been operating with known vulnerabilities as well as inadequacies.

The main threat(s) that exploited some of the above vulnerabilities in the network was the group known as Anonymous. This group was seeking retribution over two of its members having legal action taken against them. Anonymous proceeded to launch a malicious attack on the Sony PlayStation Network by way of a Denial of Service (DDoS) attack. The attack led to the exposure of the sensitive information for approximately 77 million accounts.

There were many repercussions as a result of this data breach and external intrusion catastrophe. Sony would go on to lose an estimated $171 million in costs. Service for the PlayStation Network was down for multiple weeks. Fallout was so severe Sony offered compensation to PlayStation Network users as well as faced numerous lawsuits which directly led them to alter their terms and conditions.

Sony would also go on to make changes to their cybersecurity that were deemed improvements, though arguably some changes that should have been in place to begin with. Some safety measures that are effective include – better data encryption, enhanced detection/alarm system, additional firewalls, and better employee safety training and security awareness. Once the hackers entered the system – at least encryption could have prevented them from further accessing specific information, an enhanced detection/alarm system would have detected unusual activity sooner and properly alerted analysts immediately, and better employee training will adequately educate them on better safety and security principles that will decrease threats and risks. Implementing some of the above-mentioned safety measures would have surely decreased or eliminated the risk of the eventual attack and prevent further ones from taking place.

REFERENCES

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. (2017). User Compensation as a Data Breach Recovery Action. MIS Quarterly, 41(3), 703-A16.

Bonner, L. (2012). Cyber risk: How the 2011 Sony data breach and the need for cyber risk insurance policies should direct the federal response to rising data breaches. Washington University Journal of Law and Policy, 40, 257.

Messmer, E. (2011). The Sony PlayStation Network breach: An identity-theft bonanza. Network World (Online), Network World (Online), 2011.