Sony playstation security breach

It is almost impossible to find the top reasons why most security breaches happen on a secure network compromising hundreds to thousands of users' personal information. To protect a network and thoroughly secure confidential information, one has to examine the top vulnerabilities and think outside of the normal box to protect it. When a security breach happens, there is usually a pretty simple reason why it has happened. I will discuss one of the highly publicized security breaches to happen in years, the Sony PlayStation Network & Qriocity music and video service, what caused the breach and how this could have been prevented.

On April 27, 2011 more than 70 million customers of Sony's PlayStation Network and Qriocity music service received a disturbing email saying that everything the company knew about them including where they live, when they were born, their logins and passwords, and possibly more information had been hacked into. On May 2, 1011, a week later, a second security breach occurred on a different Sony network. The Sony Online Entertainment Networks was targeted and compromised 24. 6 million users. Of that number, 12. 3 million had their credit card information stolen.

Lastly 2, 500 user's names and addresses were leaked from the electronics division of Sony creating a third incident. A total of three security breaches in three weeks amounted in over 100 million users having their personal information stolen makes customers' faith in Sony grow to an all time low. There are many issues that could have led to Sony's breach in security which include: •Deploying the right security products – IT security today has a wide range of technologies that are aimed specifically at lowering risks and threats. Coping with business growth and expansion – While companies are

acquiring others at a rapid rate of speed to drive growth for businesses, these companies are letting their information management systems lag behind in growth. •The nature of the breaches – Sony is still having ongoing investigations into why their security breach happened, application-layer attacks attributed to the first two breaches. This makes one wonder if Sony took the appropriate measures when structuring their security defenses against such attacks.

Safeguarding personal information has become more difficult than ever before with so many services on the internet that require you to enter your personal information for many reasons. Americans cannot trust companies to safeguard their information anymore because hackers prey on people and companies with weak security infrastructures. Hackers are skilled at breaking computer programs and gaining unauthorized access to the data with fraudulent intentions.

It is very unfortunate this happened to Sony because they have lost a lot of credibility with their users. The sheer magnitude of 70 million users scrambling to change their passwords, close those credit card accounts, 93, 000 user accounts were taken down because their passwords and credit card information had been stolen. Even though there are still ongoing investigations into the details surrounding the three Sony security breaches, it has been very hard to pinpoint the exact source and reasons why the breaches happened.

This has marred the public's opinion of Sony as a company. Their reputation has been scarred and it will take a lot for customer's opinion of this electronics giant to turn around. The repercussions from this are widespread

for Sony's customers. They are now subjected to identity theft, credit card fraud, and years down the road they are looking at phishing attacks because their email addresses have been compromised.