Timeline of Events :

* 2023-11-06, 06:23 PST: Incident discovered
* 2023-11-06, 06:30 PST: Incident response team assembled
* 2023-11-06, 07:00 PST: Payment processing systems taken offline
* 2023-11-06, 08:00 PST: Investigation begins
* 2023-11-06, 09:00 PST: Containment measures implemented
* 2023-11-06, 10:00 PST: Eradication measures begin
* 2023-11-06, 11:00 PST: Recovery measures begin
* 2023-11-06, 12:00 PST: Payment processing systems restored
* 2023-11-06, 13:00 PST: Notification of affected customers begins

The strike had a huge impact. The hack affected approximately 10,000 consumers and is estimated to have cost $1 million. The attack was launched because of a flaw in our payment processing systems. The attacker took advantage of this flaw to gain access to our systems and steal credit card information.

To prevent such assaults in the future, some things that can be done are to repair the flaw in our payment processing systems. Multi-factor authentication should be implemented for all users that have access to our payment processing systems. Regularly audit the security of our systems and networks. Monitor systems for unusual activity and respond quickly to any notifications. Educate personnel on best security practices.

This was a terrible situation, but you have to be determined to learn from our mistakes and improve our security posture. Steps must be taken to mitigate the impact of the assault, prevent such attempts in the future, and contact customers who have been affected.

Citations

National Institute of Standards and Technology (NIST) - Framework for Improving Critical Infrastructure Cybersecurity: <https://www.nist.gov/cyberframework>

Center for Internet Security (CIS) Controls: https://www.cisecurity.org/controls

Open Web Application Security Project (OWASP) Top 10: https://owasp.org/www-project-top-ten/

Carnegie Mellon University - CERT Division: https://www.cert.org/