PPIT ASSIGNMENT

19k-0146

ALi Hamza usmani

Q1)

Flayton Electronics was suffering from the problem of potential data theft of their customers from their stores.

Flayton Electronics was operating globally in various parts so they had a vast pool of customers so it was a matter of losing customer trust which takes time to develop.

Several fake transactions were going through their stores from stolen cards and they had no idea for some time.

Q2)

PCI(Payment card industry) defines a set of protocols which every company working on transactions has to follow to ensure security and compliance and Flayton electronics was following the PCI compliance 75% protocols prescribed by PCI.

They had their customers' information stored on-premises of their organization to ensure confidentiality of data.

It had an infrastructure consisting of firewalls to restrict access to unauthorized users.

Q3)

PCI(Payment Card Industry) provides standards for the protection of data which ensures maximum protection against possible attack vectors.

Flayton Electronics was 75% PCI compliant, the remaining 25% was still the risk that a possible cyber attack could happen.

External security audits are crucial to the data security of any large scale organization but Flayton electronics was not conducting external audits which prevented them from covering possible vulnerabilities in their system.

Their firewall was down and they didn’t know it which shows that compliance policies were not focused.

Q4)

James E.Lee(Choice point)

Their company was attacked by hackers through a fraud scheme which caused them to leak data of 145000 customers.

They notified the affected customers, set up call centers for information and offered credit monitoring services to customers.

Bill Booni(Hobby hacker)

The organization should have a senior information protection as director or vice president who has expertise in information security.

Policies and protocols are crucial to prevent risk of potential outsider attack from employee negligence.

Assemble a legal team to handle judiciary matters.

Philip Coghlan

Banks that issue payment cards are the first to identify fraudulent activities in their systems.

Should speak out to the public in case of any theft as Flayton was trying to hide the activity from their customers so the trust may be intact.

if Brett Flayton’s company provides a timely, focused, and effective response, his compromised customers might just become the most loyal of all

Jay Foley

The company’s first action must be to reduce the risk of possible thefts by eradicating any vulnerabilities in their systems.

A survey was conducted which concluded that 52% companies had experienced unauthorized access to their systems but only 15% of them suffered any financial losses.

So Flayton electronics only suffered passive attack where they were not affected financially only minor data was leaked.