K190161

Shah Tanzeel Ahmed

Section-G

PPIT QUIZ #3

Q1)  what is the issue described in this study.

Ans)

* The case study is based on a potential data theft that occurred at Flayton Electronics.
* A hard earned reputation of Flayton Electronics was at stake because of the known data breach.
* Flayton Electronics was showing up as a common point for a large number of fraudulent credit card transactions.
* The case study states how the above stated company lost its customer trust just because of the information theft of its customers.

Q2) what are the existing preventive measures at the company.

Ans)

* Flayton Electronics’ management had an obligation to make sure that it employs credible employees who will keep customers information confidential.
* Flayton made sure that its Firewall remains working throughout to avoid hacking incidences.
* All companies dealing with telephone card payments need to comply with all payment card industry (PCI) standards. Flayton Company was only 75% PCI compliant.
* Brett Flayton can hold a meeting with the major customers, explain the latest discover it has made on the security of cards, and detail any information their hands now. Any defrauded customer will protect themselves from further frauds as a result.
* Abandoning a line of business worth $20 million because of its potential to risk a future data breach.
* Changes in culture, every employee must now pass yearly privacy and security training courses as a condition of employment.

Q3)  Brief about the standard compliance issues.

Ans)

* PCI (Payment Card Industry) was a standard for data protection.
* Constantly improving your own technology makes it complicated to follow PCI compliant.
* Flayton Company was only 75% PCI compliant as per Sergie Klien, CIO. Which was not enough for a big company.
* Brett knew that PCI compliance, which was mandated by all the major credit card companies, required regular scans by an outside auditor to ensure that a company’s system were working with stiff penalties. However, they don’t scanned them every day, it was up to Sergei.

Q4) Each expert shared valuable suggestions towards the company and also shared their own story. Heading wise discuss and summarize the commentary made by the experts at the end.

Ans)

How should the Flayton electronics team respond to the crisis?

**By James E. Lee:**

* How you react to news of a security breach at your company is, as a practical matter, much more important than what actually happened.
* In 2005 our company was the victim of a fraud scheme in which criminals posed as customers to obtain the personal in- formation of 145,000 people from our data systems.
* Some of our preventive steps were radical, including abandoning a line of business worth $20 million because of its potential to risk a future data breach.
* Timing is a crucial factor in the inevitable lawsuits, which focus on what executives knew and how long they knew it before going public.
* Beyond ﬁxing the ﬁrm’s weaknesses in data security, CEO Brett Flayton must develop a brand-restoration strategy.
* The company should, as Choice Point did, notify the affected customers rapidly, set up toll-free information hotlines, and offer credit-monitoring services.
* Then they must exceed these basics with a broad range of extras to keep customers loyal: Offer discounts and sales, meet with critics of the company, and develop and promote new web pages that out- line reforms in the ﬁrm’s policies and practices.

**By Bill Boni:**

* That’s not often the case when it comes to information security, including prevention of and planning for data theft. “Let the technical staff handle that” tends to be the default strategy, with responsibility relegated to non-senior IT or corporate-security management.
* Businesses that are serious about protecting their data and preserving the data’s value should have a high level ofﬁcial, such as a director or a vice president of information protection, who serves not merely as a man- ager but as a senior champion in this area.
* Also beneﬁcial are policies, procedures, and training protocols that are customized for each company function, to reduce the likelihood that individuals will make wrong choices because they do not under- stand how the overall data standards apply to their speciﬁc roles.
* During my tenure in information security, hobbyist hacking has evolved to become a much more sophisticated, parasitic extraction of valuable data from targeted organizations.
* You can assemble an internal team of lawyers, accountants, and experienced digital-forensic investigators from law enforcement or defence agencies or use external sources such as law ﬁrms, public accounting ﬁrms, and consultancies with digital specialization.

**By** **John Philip Coghlan:**

* Banks that issue payment cards, such as the ﬁctional Union Century, are often the ﬁrst to spot possible fraud when their systems identify merchants who are common points of purchase for potentially compromised accounts.
* Beyond the institutional stakeholders just described, there are consumer groups, legislators, shareholders, and of course the employees and customers, whose interests we see Brett Flayton actively considering.
* If he doesn’t speak out, he is not allowing his customers the best means of protecting themselves: by using a different, uncompromised payment card or by scrutinizing transactions on the compromised card.
* Among the potential avenues are to use contact information from the store’s own database; to set up a special company web page; and to hold exclusive informational events, such as call-ins and webcasts, all reinforced with a customer support hotline.
* So, if Brett Flayton’s company provides a timely, focused, and effective response, his compromised customers might just become the most loyal of all.

**By Jay Foley:**

* Someone else in the transaction chain, such as the credit card processing company, might very well be at fault, in which case it would be wise to wait for that party to come forward ﬁrst.
* The company’s ﬁrst action should be to reduce the risk for future thefts by closing any data- transaction loopholes that this incident has brought to light, provided that the Secret Service does not think it will interfere with their investigation.
* In 2006 the Computer Security Institute in San Francisco conducted a survey of 616 large, U.S. based companies and found that 52% had experienced some kind of unauthorized use of their computer systems.
* From the Computer Security Institute, we have the ﬁgure that only 15% of their surveyed companies suffered ﬁnancial losses as a result of cyber security breaches.
* We also know that most victims of data theft do not then become victims of identity theft.
* In fact, it’s likely that customers at Flayton’s were victims of this type of fraud.