# INFORMATION SECURITY CASE STUDY

Name: Pavan R Kashyap SRN: PES1UG20CS280
6th Semester E section

**Q1. What is your diagnosis of the breach at Target—was Target particularly vulnerable or simply unlucky?**

**Answer:**

Target was particularly vulnerable to the breach. The breach was carried out during the peak buying season (Black Friday time period). Companies must beef up their security measures especially during the peak season, for this is the time that they are most susceptible to attacks. However, Target did not do so.

Target allowed its vendors (Fazio Air conditioning services) direct access into its unsegmented network. Access control on who has access to what, was not practiced by Target. Even though Target's computers/ network was never directly attacked, the attackers were able to route themselves into the network via the compromised vendor's credentials.

Target failed to ensure that its vendors follow the principle of least privilege (they have access to only required data) and practice two-factor authentication. This made the network and the devices connected in the network(POS systems) vulnerable to an external attack. In some senses, we can attribute the vendor access to the entire network as the weakest link in Target's defence planning.

Target received repeated warnings from FireEye stating that there was some malicious activity in the network. These warnings were ignored by Target, stating that they were merely false positives. Target had the opportunity to detect and prevent the attack; however, its lax nature prevented it from doing so.

It is also made clear by the audit team that the functionality to detect and delete malware was turned off in Target's systems. This causes the malware to reside on the POS systems and extradite all credit card details to the servers on the network(and eventually to the attacker).

It is also stated that two months prior to the attack, Target's in-house security team stated that there are certain vulnerabilities in the POS system. They also asked them to review the payment network. However, these requests were never followed upon – Target was preparing for a heavy traffic weekend (heavy sales).

The points stated above show how Target made itself highly vulnerable to an external attack. It can be agreed upon, that Target was unlucky, but this idea only stems from the fact that Target made itself vulnerable.

# INFORMATION SECURITY CASE STUDY

Name: Pavan R Kashyap SRN: PES1UG20CS280
6th Semester E section

**Q2. What, if anything, might Target have done better to avoid being breached? What technical or organizational constraints might have prevented them from taking such actions?**

**Answer:**

It makes sense for Target to prioritise other non-functional requirements during the peak season, like scalability and performance, however ignoring security concerns is not correct. Target must have beefed up its security measures in advance, so that prioritising other requirements would not have compromised the core security requirement.

Target's in-house security team suggested changes to the network only two months prior to the attack. Limited time did not allow Target to fully focus on the security concerns of the POS systems. The security team must have been more pro-active and monitored and reported these concerns much earlier. Similarly, the organization could have employed a larger work force to fix the issues with the payment network, without disrupting other actions and services.

Target must have segmented its network much earlier. It should have kept the payment network away from the network directly accessed by the 3rd party vendors. Segmenting a vast network is a daunting task, no doubt; however, the organization could have started the segmentation/partitioning slowly (one location/ section of locations) at a time.

There is no mention of any defence in depth mechanism used. Target should have used several internal firewalls, updated anti-virus software and IPSs to protect one internal network from another (in case one of the networks is compromised).

Two factor authentication, if employed would have made it more difficult for the attacker to enter Target's network. Although it is difficult, it is not impossible. Compromising the user's device can help the attacker travel past the two-factor authentication too.

The organization's security team is not autonomous in true sense; no action is carried out until orders are received from those high in the hierarchy (CEO and the board of directors).

Even though warnings were provided months before, and when the malware was ready for installation on the systems, there was no 'Go' message provided by the management to immediately tackle the issue. The organization's leadership did not consider security a primary concern; they were more concerned with keeping up with the increased traffic.

This organizational constraint restricted the organization from detecting and preventing a breach early on.

Majority of the tasks suggested above are all cost intensive in nature. They require a huge work force to be active and operational, working round the clock. Deviating revenues into improving the security of systems, may not have appealed to the management. Partitioning the network needs technical experts. Implementing firewalls, deploying an IPS all need network resources, funds, and time. Target may not have possessed the required skills (and/or funds) to operate on the same.

These technical constraints restricted the organization from preventing the attack in the first place.

**Q3. What is your assessment of Target's post-breach response? What did Target do well? What did they do poorly?**

**Answer:**

Target faired reasonably well initially, until everything went downhill. Target sent out a brief stating that it was aware of the breach and that it had alerted the Govt. institutions on the same. They offered free credits and provided theft monitoring services to their clients for a year. Every organization cannot disclose details of the attack openly initially, for they will fall under heavy media scrutiny. Any unnecessary panic created by the media can in turn affect their customers. Target chose to stay fairly silent until it had gathered all details pertaining to the intensity of the attack. Assurance by the CEO that SSNs and PIN numbers had not been compromised, ensured that customers did not go into a panic frenzy. However, things started to get messy after this. They even provided discounts to placate the worried customers; they wanted to restore some sense of normalcy.

Target did not set up sufficient help lines to cater to the panicking customers. The services they provided to their customers in time of need, was poor and ill-equipped. Customers were unaware on how they could solve the problem of fraudulent transactions. Target should have collaborated with other card service providers and released circulars to customers on how best they can protect themselves from the damage.

The CEO retracted his original statement days later, claiming that PINs were compromised and that the breach was larger than they initially expected (70M). Although, this honesty must be appreciated, it tainted Target's image as it painted the CEO as a hypocrite. Although the CEO apologized for the long wait times and claimed that they were working on scaling, it never translated into results.

Target's PR and legal team might not have been ready for what ensued. Once the breach was reported and disclosed in public, Target should've immediately deployed its PR team to work on damage control. The greater the media fire, the more damaging it is for Target.

**INFORMATION SECURITY CASE STUDY**

Name: Pavan R Kashyap SRN: PES1UG20CS280
6th Semester E section

Target did not work on defending and saving its face in the public frame. Target paid hefty lawsuits to customers and banks. A powerful legal team and a legal win could have saved Target from media's brunt.

**Q4. To what extent is Target's board of directors accountable for the breach and its consequences? As a member of the Target board, what would you do in the wake of the breach? What changes would you advocate?**

**Answer:**

The failure of a team is generally attributed as the failure of the team leader; the success of the team is attributed as the success of all the teammates.

This is a general belief, although I do not endorse it strongly. In public perception, if anything goes wrong, then they need someone to blame—it is usually the leader who manages and supervises the working of the team. The leader leads the team and paves the path for the team's progress. Anything that hinders it is considered the fault of the leader's skills and ideologies.

The same applies to our case at hand. In true sense, the board of directors were never actually involved in the attack in any way. They were unaware of the vulnerabilities (possibly) in the organization and their role was to merely ensure that the organization works seamlessly. They work with the company's stakeholders to ensure that the company is on track. They do not supervise the working of the day-to-day activities of the various departments in the organization. So, to a certain extent it is reasonable to state that the board must not be held accountable for the faulty, flawed structuring of their departments and employees.

However, as discussed above and previously, every action having certain consequences must be taken by the management (CEO and board). The primary roles of the board include risk management and compliance assurance. The organization reported the vulnerabilities regarding the POS systems and indicated how the compliance certificate obtained was not up to the latest standards. These two points fall in the purview of the day-to-day activities of the board. Their inaction indicates that they were lax in their duties and thus, indicates that they were responsible and accountable for the breach and consequences (more than they were not).

Pacifying the customers and ensuring that my network is sanitized and safe (free from malware) would be my foremost goal if I was a member of the Target board. I would

summon the incidence response team and connect with forensic tools to identify and clear the breach as quickly as possible. Assessing the damages would give me an estimate on the extent of the attack. I would ensure that a public statement is made quickly, but with sufficient knowledge on what has happened. Resources would be dedicated to scaling up "Customer service", so that customers do not feel cheated or betrayed in the wake of the attack.

There was nothing substantial done for the customers. I would change this and ensure that my priority is customer safety. If I lose my consumer base, then my organization is bound to close. I would ensure that circulars are released on a frequent basis to indicate to my customers on the things they can do to protect themselves.

I would not quote any statistical figures until the investigation is done and I would ensure that details of the breach are told to individuals on a need-to-know basis.

**Q5. What lessons can you draw from this case for prevention and response to cyber breaches?**

**Answer:**

This case makes it amply clear that "prevention" is the key. Ensuring that the organization's network and its devices are secure is of at most import. Security can sometimes get side lined because of other responsibilities, but the effects of side-lining security can be very damaging. The case study also makes it clear how merely generating a security policy is not sufficient; its implementation and pro-active refinement is essential.

Having professional security experts who are well-qualified is important – in the board as well as in the Incidence Response teams. Network segregation/segmentation must be followed as a mandatory security principle to prevent compromise of the entire organization network layout.

Although false positives are common, security monitoring messages must be verified before dropping/discarding them, because there is a possibility that a valid response may be hidden/supressed within several false positive responses.

Security related activities must be taken up earlier, if it is believed that it may not be given the attention it deserves in the days ahead (the Black Friday sale in our case).

Anti-virus software must be up-to-date. Firewall rules must be written in compliance with the security policy with "default deny" as its behaviour, should it fail.

Delegating duties and assigning specific roles (like the CIO) is important.

These are the lessons that need to be employed to prevent a cyber breach.

Name: Pavan R Kashyap SRN: PES1UG20CS280
6th Semester E section

Active response is most essential. The organization must actively understand and mitigate the breach as quickly as possible. Whilst doing so, the extent of confidential information loss must be assessed. The servers must be sanitized and brought back up quickly, so that normalcy returns. The quicker the mitigation, the better prepared the organization is.

The management must take the front role at times of crisis and provide all the required facilities, funds and resources needed for the mitigation. Ensuring that all the departments involved work without conflicts is another task that must be upheld.

The stakeholders involved must be contacted as part of the response; effort must be made to ensure that the damage caused to them is as minimal as possible. An audit team must be contacted and brought to the location. Government agencies must be notified, so that they can in turn provide some form of assistance directly or indirectly.

Litigation and media scrutiny is a consequence that follows an attack. It cannot be entirely avoided, but the organization can make some effort to minimize the damage.

**Q6. How would you characterize your role as a director in relation to cybersecurity at your organization? What are some concrete things that you can do as a director to oversee this domain?**

**Answer:**

Cybersecurity must be one of the essential aspects of the organization (and board of directors). As a director, I would ensure that I oversee what the cybersecurity risks are, and how best I can manage them. I would ensure that I am pro-active and approachable. I would take an active part in understanding what the shortcomings are, and how best we can solve them in a cost-effective way. Every minute activity does not need direct reporting to the director; I would designate an elaborate hierarchy that is capable of handling this.

As a director, I would first ensure that an elaborate security policy is created that complies with the company culture of the organization. Everyone (irrespective of whether they are employed under Cybersecurity department or not) must follow certain security standards and guidelines to ensure that the organization is safe from within. In order to so, training and awareness programs will be carried out to ensure that all employees are aware and well-equipped (to follow safe coding practices and tackle social engineering problems).

Subsequently, I will also ensure that all the resources needed by the Cybersecurity department are made available to them as quickly as possible. These can include compute resources, certain new technology, certain tools. It also includes funding. I will vouch for

greater allocation of funds to the security department, in the board meetings, so that the organization is up-to-date and prepared to tackle any cybersecurity attack.

I will review cyber security performance reports of past incidents to see how better/ill equipped we are to handle cyber-attacks. The analysis of our past incidents will provide us a picture of what was done right and what needs to be done right. This will provide a direction for the department to work in. These incidents do not necessarily need to be damaging incidents; minor attempts at infiltration also indicate how prepared our network and devices are.

I will also ensure that I am adequately aware of the risks that my organization will face and the consequences that the company might have to face, should a damaging breach occur. This will motivate me to stay pro-active and in-touch with my organization's cybersecurity status.

**Q7. What do you think companies can do better today to protect themselves from cyber breaches and in their post-breach response?**

Companies must firstly invest in firewalls and IPS systems. They must ensure that they have the latest technology inducted into them. Every day, new vulnerabilities are being discovered (and attackers are creating new variants of malware). So, companies must ensure that their IPS and anti-virus systems use updated datasets (with updated hashes and malware signatures). The organization must regularly assess their preparedness/readiness and work on the areas where they are vulnerable.

Companies must also ensure that their systems are resilient and fail-safe/fault tolerant.

Companies must train their employees to identify cyber threats/attacks. They must educate their employees on the dangers of social engineering, phishing etc.

Companies that store sensitive information must practice defence-in-depth. They must create back-up copies of certain core information and store them in a remote location.

Companies can employ VPNs to allow their employees to access the organization's network from their homes. This ensures that employees do not directly access the network (if the employee's system gets compromised, then the organization's network could be breached as well).

Regular auditing can help the company identify any vulnerabilities that have been overlooked by the in-house security teams (Red, Blue, Purple teams).

Companies must consolidate and develop a detailed incidence response plan that indicates what set of actions/steps will be taken in case of a security breach. This ensures that the post-breach response is agile and hassle free.

**INFORMATION SECURITY CASE STUDY**

Name: Pavan R Kashyap SRN: PES1UG20CS280
6th Semester E section

Clear cut division of duties is essential in organizations. Roles must be assigned (the Incidence Response team, the Chief Information Officer etc.) and their responsibilities must be clear and well-defined. This ensures that during the post-breach response, those working on mitigating the attack know who to contact/who to delegate work to/who to work with.

Companies can consider using encryption tools/mechanisms for message passing. Network logs (and system logs) can be considered, if the organization can afford it. This will make analysis easier if there is a breach (from within or from outside).