IPB Paper

Aim Point has over 2,000 stores, located in all 50 states as well as the DC area and uses 40 distribution centers nationwide. They are a general merchandise retailer employing 333,000+ employees. ¾ of the US lives within 10 miles of an Aim Point store. Since August of 2016, the CEO of Aim Point has been Seymore Proffets, who is very active on the political scene and donates 10% of the company profits to charity. Routine business operations are managed from a dozen offices, the national headquarters being in Denver, CO. Aim Point Corporation also owns Wombat Holler Country Store.

Given the size of Aim Point Corporation, physical security at all locations is very well managed. All building entrances have adequate lighting, are covered by cameras, and require code or key entry. The store, business offices, and distribution centers have security systems in place which are only accessible by specific employees. Each employee has their own security code to access ‘Employee Only’ areas and to clock in and out each day. All locations have a server room that remains locked at all times, unless the contracted IT company is performing maintenance. There are also cameras continually monitoring throughout the store and distribution centers. Given that the distribution centers contain a lot of products, Aim Point contracts out security guards to patrol the building periodically throughout the day and night.

Theft of physical items by staff or customers, data breaches, inventory damage, data theft, customer injuries, blackouts, competitors, forced closures (such as a pandemic), and impeding product shipments are just some of the things that could affect this business. There is also the fact that the CEO, Mr.Proffets, is active in the field of politics which opens the door to a lot of scrutiny. While some of these are more likely to happen on a regular occurrence, some would make a larger impact than others.

The largest threat from a cyber perspective would have to be data breaches and theft. This can be done from an outside or inside source and would create quite an issue for the company whether they are stealing financial information from the customers or looking for data to use in a political power move. The second largest threat would be physical theft. Creating an environment that is deterrent to thievery is key. This requires appropriate security in both the physical and cyber realms.

Course of action for the first threat would be ensuring that all employees are receiving fair compensation and care to ensure that they are happy and less likely to assist any adversary looking for a way in. You also need to constantly monitor and record all data coming through your business. This can be done with a SIEM with the appropriate amount of cyber security staff and alerts. Each location’s server room should be locked at all times and routinely checked for ‘additional’ hardware that may have been installed by an adversary. With the influx of online shopping that has occurred with the COVID-19 pandemic, there needs to be constant monitoring on that front as well. Courses of action for the prevention of physical theft would be security teams located at all warehouse locations, monitoring and electronically logging who comes and goes, along with doing routine checks throughout the building. There would need to be security systems at all locations as well, to include cameras. We would also need to accurately log each item as it enters and leaves each facility with extra care being taken for those high dollar items.

Overall, there are many things that could affect Aim Point stores, offices or even simply its reputation. With the appropriate security measures in place there are many things that can be done to prevent these issues, keep daily operations going, and protect not only the company, but its customers.

Bibliography

1. <https://www.inc.com/encyclopedia/office-security.html#:~:text=Office%20security%20can%20be%20broken,inside%20the%20company%20and%20out>.
2. <https://www.thefulfillmentlab.com/blog/warehouse-security>
3. <https://www.insureon.com/blog/retail-risk-management-the-top-threats>
4. <https://www.itpro.com/security/cyber-security/360747/why-retailers-are-the-most-targeted-sector-for-cyber-attacks>