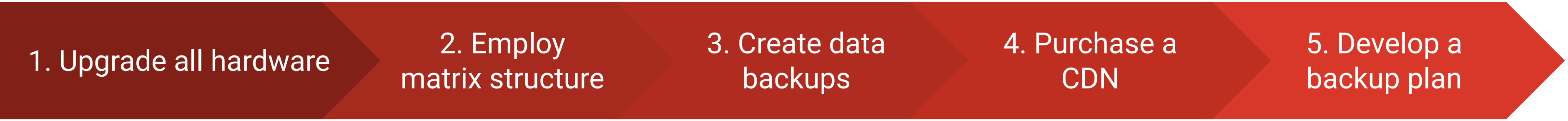

1. Upgrade all hardware

2. Employ matrix structure

3. Create data backups

4. Purchase a CDN

5. Develop a backup plan

Suffolk County’s current computer systems are outdated and susceptible to attacks. Their first priority should be to upgrade all outdated hardware to newer technology. They must also invest in stronger firewall systems to prevent their networks from being infiltrated.

Suffolk County’s functional management structure has been very ineffective. Employing a matrix structure will allow for the overseeing of company processes, and will ultimately improve the communication channels present within the organization.

Four terabytes of Suffolk County data was encrypted during the cyberattack. As a result, they lost a significant amount of company data. Moving forward, all company and client data must be backed up weekly. In addition, Suffolk County should invest in cloud infrastructure for further data backup.

Inability to access county systems, networks, and data was one of the largest issues resulting from the cyberattack. Investing in a CDN from Cloudflare would help protect Suffolk County from future attacks, and ultimately ensure availability of all company systems, networks, and data.

Suffolk County did not have a disaster plan to fall back on for when an attack occurs. As a consequence, they struggled to deal with the effects of the cyberattack. Suffolk County should develop a backup plan outlining the steps that must be taken for any future attacks that occur within the organization.