December 25th, popular UK based retail chain, ASOS is struck by a double-extortion ransomware attack. The cause of this attack upon later investigation was an exploited vulnerability on a Microsoft Exchange Server, leading to the compromise.

The attacker's are threatening to leak consumer credit card data, personal details, and company data unless a hefty ransom is paid before the new year. Due to the holiday, the company was only made aware of this breach about 12 hours after the breach occurred, and have now reached the "crisis defined" stage of the cyber attack. Again, due to the time of the attack, the company unfortunately has not had enough time or designated spaces to make new, secure backups of the affected data. The company due to the lower workforce, and refusal to oblige by the attacker's demands, has its data leaked on the first of January. The company after regaining control of its systems, phase 4 of cyber operations, begins wiping drives and reloading backups of systems before the initial breach occurred. The company waits to notify victims and the public of the breach until the middle of February, to not cause undue panic and to gather accurate information on those affected.

This breach ends up costing ASOS and U.K. citizens around 300 million pounds.

Retail based companies are usually only able to apply a few phases of cyber operations and never the whole thing. Retail companies can only apply phase 0 - prevent and prepare, phase 1 - crisis recognition, and phase 4 - stabilization. Even then, these phases are a lot more general than the other phases of cyber operations, so they can be applied to almost any cyber attack. All cyber operations defined in the military sphere are extremely defined, and strictly regulated for cyber warfare and military cyber attacks, and as such cannot be used for non-state cyber attacks on retail businesses. However, if it is found that a U.K. retail company is attacked by a state-sponsored breach, then it becomes a matter for the U.K. government as a potential act of war. Again, if you think about it, a retail company recovering from a cyber attack should not worry about dominating forces and full spectrum control, or leaving things to civil authority.

For ways to prevent ransomware attacks like these in the future, let's look back into the ASOS scenario. The cause of the breach was due to a Microsoft Exchange Server vulnerability, which under further research, has been the cause for over 30,000 compromises in the U.S. alone since March 2021. The company had no strict regulation over emails sent using this service, and as a result a phishing email made to look official eventually got through. The company then had no routine backups or secure off sites for backup data to be held. And as a result, were ill prepared for when breached. The company as a whole did not do any of phase 0 of cyber operations - preventing or preparing for cyber attacks. I would personally recommend proper planning for attack prevention, such as routine updates, employee training, and accurate system monitoring of all potentially vulnerable software or assets. As cyber attacks are inevitable, proper planning for the aftermath of these breaches would see information gathering be smoother, consumers to be notified sooner, and for systems to be online and normal sooner.

References

https://www.marketplace.org/2017/09/11/why-do-companies-wait-so-long-tell-us-weve-been-hacked/

https://eandt.theiet.org/content/articles/2021/11/ransomware-now-cyber-criminals-weapon-of-choice-as-uk-retailers-face-barrage-of-cyber-attacks/