A Grade Round 2

That we should hold company directors & CEOs criminally responsible for security breaches (e.g. data breaches).

Background:

With the increasing dependence on digital technology, cybersecurity breaches have become a significant concern, which could lead to service disruptions and exposure of sensitive data. Some raise a solution: company directors and CEOs be held criminally responsible for such incidents. They argue that this would encourage businesses to invest more resources in enhancing cybersecurity measures. Additionally, such penalties would align the corporate world with other industries, such as aviation or food safety, where negligence can lead to criminal consequences.

However, opponents argue that this measure could be unfair and counterproductive, as not all security breaches result from negligence. Holding company directors and CEOs criminally liable could discourage talented individuals from taking such roles.

Questions for consideration:

- Would this policy encourage companies to invest more in cybersecurity training, systems, and staff?
- How can criminal consequences ensure a higher standard of corporate governance and ethical responsibility?
- Would this policy encourage better security practices, or would it unfairly penalise executives for factors beyond their control?
- Should companies be incentivised to improve security in other ways, such as fines or mandatory audits, rather than criminal charges?

Resources:

https://ia.acs.org.au/article/2021/hold-company-directors-liable-for-cyber-attacks.html

https://duo.com/decipher/gartner-warns-ceos-will-be-personally-liable-for-breaches-by-2024

https://www.nortonrosefulbright.com/en-au/knowledge/publications/b0dae4a0/cyber-risk-and-directors-liabilities-an-international-perspective