HRIS CASE ANALYSIS

Submitted by

TARUNI JAIN[21PGDMHR32]

Submitted to

Prof. Prerna Lal

Of

PGDM-HR(2021-23)

Introduction and Premise

In January 2010, Malcolm Harkins, Intel Corporation's chief information security officer, faced difficulties in pushing forward with the BYOD project. According to Gartner Inc.'s IT Glossary, Bring Your Own Device, or BYOD, is an alternative strategy that allows workers, business partners, and other users to execute workplace programmes and access data using a personally selected and purchased client device. It's possible that a subsidy will be added. For over a year, the company's IT section had been driving this programme. Harkins was charged with coordinating the initiative's introduction across the organization after upper management chose to make a strategic decision in favor of embracing BYOD.

For dealing with bring-your-own-device situations, the organization had three options:

- Intel's first option was to do nothing and assume that the fad of people bringing their own devices to work faded away. The status quo would have been preserved, but IT activities outside IT management, or "shadow" IT, would have been forced even further into the shadows.
- Another option is that the company has said unequivocally that BYOD is not permitted. In this plan, Intel would have control of all IT equipment used in the company as well as organizational oversight, resulting in a consistent technology implementation across the board. On the other hand, making this decision may cause the company to lag behind recent trends and alienate a portion of its personnel.
- Finally, Intel may encourage bring-your-own-device (BYOD), a sensible approach based on a set of unbreakable "laws." Compromises with personnel are inescapable for CIOs (chief information officers) in this situation. They lack the ability to enforce their own rules.

The dilemma

How could Intel make Bring Your Own Device (BYOD) work for them? For a variety of reasons, the panel unanimously determined that this was the problem, the first of which was that, as mentioned in the case, Intel's top leadership had already made a strategic choice in favour of adopting BYOD. Second, according to the lawsuit, Harkins was appointed to head the BYOD project execution owing to a choice made by high management, and he had previously developed strategies, frameworks, and a risk management model. Another factor is that more people are using their own devices for work.

Arguments in support of BYOD

- Less hardware and IT support cost

- Reduction in HR expenses
- Better place to work
- Low customer lead times
- More efficient workflow
- Higher productivity

Arguments against BYOD

- Security risk and privacy issues on unmanaged devices
- Co-mingling of data
- E-discovery

Options for a implementing a categorical "NO":

- The company will only allow certain devices (CYOD):There will be some commonality among the gadgets used for company-related duties. CYOD also gives Intel the benefit of knowing how to troubleshoot and respond to difficulties because of its familiarity with the device. Additionally, the apps must be checked and approved before Intel staff may install them on the devices.
- Only select employees are allowed to bring their own devices, which has the advantage of giving a better degree of control than if all people were given the option. There are a number of other disadvantages to choosing this option. First, some employees may experience resentment if they are not chosen. This may result in a rise in the number of employees seeking a more flexible work environment. This, too, may act as an incentive for people to hand out personal information to strangers or hackers in unethical and illegal ways. There may also be concerns with the devices that these employees utilise, such as those provided by Intel, in terms of comfort and flexibility.

Options for implementing complete BYOD:

- If desired, employees will be permitted to bring and use their own devices: Intel will be unable to consistently check the cybersecurity of diverse personal devices as a result of this decision. In terms of information security, the company would have a hard time establishing a common foundation for the numerous lines of personal electronics.
- Employees will be required to bring their personal devices to work: This choice has both good and bad implications for the company. On the one hand, this option has the benefit of increasing employee productivity. Employees who desire to keep their professional and home life separate may protest this. Another cause could be that some employees are unwilling to hand over their personal devices to the IT team or the company.