



HRIS CASE ANALYSIS

Submitted by

ADITYA NARAYAN RAY[21PGDMHR03]

Submitted to

Prof. Perna Lal

For

PGDM-HR(2021-23)

Introduction

Malcolm Harkins, Intel Corporation's chief information security officer, had challenges in moving forward with the BYOD project in January 2010. Bring Your Own Device, or BYOD, is an alternative strategy allowing workers, business partners, and other users to execute enterprise applications and access data using a personally selected and paid client device, according to Gartner Inc.'s IT Glossary. A subsidy may be included. This programme had been driven by the company's IT division for about a year. Because top management had decided to make a strategic choice in favor of implementing BYOD, Harkins was tasked with leading the initiative's launch across the company.

The company had three alternatives for dealing with bring-your-own-device (BYOD):

- The first alternative was for Intel to do nothing and hope that the trend of employees bringing their own gadgets to work would fade away. The status quo would have been maintained, but IT activities occurring outside of IT management, or "shadow" IT, would have been pushed farther into the shadows.
- Another possibility is that the corporation has issued a firm "No" to BYOD. Intel would have ownership of all IT equipment utilized in the organization as well as corporate oversight in this strategy, resulting in a consistency of technology implemented across the board. Choosing this choice, on the other hand, might cause the company to fall behind current trends and alienate a segment of its workforce. IT mobility was a growing phenomena, according to Gartner and McKinsey studies.
- Finally, Intel may promote BYOD, a sensible solution based on some indisputable "rules." It is unavoidable for CIOs (chief information officers) to make compromises with employees in this situation. They are incapable of enforcing their own rules.

Problem statement

How could Intel effectively implement BYOD? The panel unanimously agreed that this was the issue for a variety of reasons, the first of which was that, as stated in the case, Intel's senior management had already made a strategic decision in favor of deploying BYOD. Second, the case said that Harkins was assigned to lead the implementation of the BYOD project due to a decision made by senior management, and that he had already devised strategies, frameworks, and a risk management model. Another reason is that people are increasingly using their personal gadgets for work.

Advantages of BYOD

- Reduced hardware, IT support and human resource costs

- Increased productivity among employees
- Faster customer response times
- High operational efficiencies
- Better brand equity and employer branding

Disadvantages of BYOD

- Unmanaged Devices Pose Security and privacy risks
- Security risks of integrating global IDs into corporate data directory account
- Data co-mingling
- E-Discovery

Alternatives for a categorical “NO”:

- Only particular devices will be allowed by the company (CYOD): There would be some sort of standardization among the devices used for company-related tasks. .Because of its experience with the device, CYOD also provides Intel the advantage of understanding how to troubleshoot it and respond to issues. Additionally, before Intel personnel may install the apps on the devices, they must be examined and approved.
- Only certain employees are allowed BYOD: This has the advantage of providing a higher level of control than if all employees were given the option of bringing their own devices. There are other drawbacks to selecting this option. First, if they are not chosen, some employees may feel animosity. This could lead to an increase in the number of employees looking for a more fluid work environment. This, too, may serve as an incentive for individuals to give details to outsiders or hackers in unethical and unlawful ways. There may also be issues with comfort and flexibility in the devices that these personnel use, such as those given by Intel.

Alternatives in support of BYOD:

- Employees will be able to bring and choose their own devices if they so desire: As a result of this option, Intel would be unable to uniformly check the security of various personal devices. In terms of data security, the corporation would have a difficult time creating a common ground for the various lines of personal gadgets.
- Employees will have to mandatorily bring their own devices: This option has both positive and negative consequences for the firm. On the one hand, the advantage of this choice is that staff productivity will grow. Employees may object to this because they want to keep their work and personal lives separate. Another factor may be that some people are hesitant to handover their personal gadgets to the IT department or the firm itself.