Exercise: Security Economics & Entrepreneurship
(Adapted from an exercise in 'Economics of Security' by Angela Sasse and Adam Beautement at UCL)

Part A - ACME Water Sturminster

ACME Water operates a water treatment plant and customer operations centre in Sturminster in Dorset. The site currently has 100 staff, across customer billing and water treatment operations. The Sturminster site building is two buildings. Building A contains the main plant, some staff offices, and a meeting room. Building B is spread over 2 open plan floors, with the top floor dedicated to managers and meeting rooms. Staff are allocated specific areas in the open-plan floors, and there are an additional 10 "hot desks" for visiting staff from other sites.

Reception staff at Sturminster are responsible for screening visitors and providing access to the site. There are 2 security guards, Steve and Jim, who patrol the site regularly. There have been incidents of visitors walking unescorted into the site; when questioned by the security guards, it is usually found that they are going to meet with someone in the building. Occasionally, though, the employee the visitors are going to meet are not actually on site at that time, and have to be escorted out.

There have also been more serious incidents. Last month, Jim found a visitor checking his email on an employee's computer in Building B, which he had found unlocked and was using without permission. The week after that, two thieves dressed as cleaners managed to enter Building A during lunch hour and steal two laptops. One was owned by an instrument technician, and contained sensitive information enabling access to unmanned sites. The other contained personal information about students living in Bournemouth. As a result of this data breach, the company was fined £80,000 by the ICO.

It is quite common for staff to leave their computers unlocked when they are away from their desks and, after discussing the incidents, it was felt by business managers that this created the potential for unknown individuals to enter the site and access machines without restriction, potentially causing another data leak.

To prevent any risk of leaks and future fines, ACME staff were asked to be more vigilant, and IT managers configured all fixed computers and laptops to automatically lock their screens after they have been unused for 60 seconds.

Questions

1. Are there any potential problems associated with this policy?

The problem with the policy is that it doesn't really address all the implied risks. It seems to address the issue of intruders getting unauthorised access to email on employee computers, but it doesn't help address the problems with laptop theft or personal data breaches.

2. What costs will there be for the staff? For the company?

- *Individual costs include the physical and cognitive effort of entering passwords for <u>some</u> users, but perhaps not all, e.g. reception and call centre staff. These perceived costs could lead to "fixes" / coping mechanisms by affected staff.*
- *Individual benefits aren't so easy to spot, but it can be useful to think of the threat model faced by different users. For example, receptionists might legitimately be concerned about unauthorised access to email if they are away from their desk more than other users, particularly if they have some experience of the threat. If users see the benefits then the perceived costs could be lower.*
- *Organisational costs include the configuration of the control mechanism, particularly if they will customised by role.*
- *In terms of organisational benefits, the mechanism is a weak control for laptop theft given the screensaver could well be on when the laptop is stolen. This is unlikely to impress the ICO if the laptop contains personal data though….*

3. How effective will the policy be?

It might be workable for certain 'knowledge worker' roles or managers that spend long periods away from their workstation. However, it's unlikely to be effective without additional controls too.

4. Considering the value of the assets, how good is this policy?

This seems ok for fixed workstations, but not so much for laptops. The key challenge seems to be getting staff to be more vigilant.