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?
2. What costs will there be for the staff? For the company?
3. How effective will the policy be?
4. Considering the value of the assets, how good is this policy?

Part B - A rethink of site security

The screen-locking policy was not well received by ACME Water

Barry, Instrument Technician, 47
My job requires me to read a lot of machine specifications while I'm on the job, both on and off-site, and then look things up on my laptop. I know it's important to be more secure, but I find it very difficult to focus now...every time I turn back to my laptop, the screen has locked and I have to log in again. I try to remember to move the mouse a bit so it doesn't lock, but I still think I must have to log in about 20 times a day!

Sarah, Customer Billing, 27
At first I found the screen locking so quickly quite frustrating...every time I went to talk to a colleague, I'd come back and my screen would be locked. But I discovered that if I put a book on my keyboard then it doesn't lock. It saves me a lot of time—probably at least 15 minutes a day—and I've never seen any strange people wandering around this part of the office, anyway.

In response to complaints from the staff, the site manager has agreed to consider alternative options.

Questions

1. Using one or more of the security entrepreneurship techniques described in the lecture, elicit requirements for a practical authentication solution.