Privacy at Work: 5 Employee Policies To Prevent a Breach

Author : Cat

Date : January 26, 2020

With rising rates of cybercrime, the most likely cause of a privacy breach is still error, or lack of awareness, on the part of the employees. Though there is certainly a place for technology and tools to guard your castle, here are five policies that will keep one of your employees from accidentally leaving a door open.

Password Policy

The most tedious policies for employees but one of the most important. Programs that crack passwords are readily available and very efficient. You want passwords that have combinations of numbers and letters, and that are NOT dictionary words. I like to use common saying or titles. Ex. Three blind mice (See how they run) could become "3BM3BMShtr". When Equifax was breached, their user name was "Admin" and their password was "Admin". Makes for an easy login AND and a easy hack. This policy should, at minimum, ask for complexity requirements, but can also include how frequently it should be updated.

Personal Device Policy

It would be surprising if an employee didn't carry their own phone with them at work. The problem here is that personal devices have sketchy privacy settings that are designed to maximize data input including through a user's microphone and/or camera. If you have sensitive data in your company, ensure that this policy states that either employees' microphones have to be completely off (especially assistants like Siri) or devices should not be brought in to rooms where confidential information is shared. Same goes for cameras. Employees should not be allowed to take personal photographs within company walls lest they accidentally capture and share confidential information in the background.

Portable Device Policy

If employees use laptops, USB drives or other portable devices, ensure that you have a policy protecting access to these devices. Any device containing private information should be password protected and in the case of laptops, have the machine lock down when not in use. These devices should not be left where non-authorized persons may have access to them.

Additionally, this policy should prohibit the opening of foreign devices within your company's firewall. A dropped USB drive is an easy way for a criminal to gain access to your system when the unsuspecting employee plugs it in to see what is on it.

Business Email Policy

A great way for social engineers to work their way in behind a firewall is to get access an employee's direct email addresses. This is often done by scanning the internet for the company extension via forums, comments, or other public sites. Business emails should only be used for business purposes, not logins for social media sites. Decide if it also makes sense to limit use of that email on shared knowledge sites such as github.

Clean Desk Policy

Access to printed documentation should also be protected, it may be in relation to clients/users/customers or other employees. If a document is not in use it should be locked up. Private data should never be left on a desk where it could be seen by a visitor or even an unauthorized employee.

Don't let a lack of understanding put your company at risk. Education is key to a culture of privacy. Ensure you include these policies in your onboarding and remind current employees on an annual basis.