

If I owned a company, I would make sure that all employees that are outside of the IT department are capable of learning the basic cyber security practices. I will make sure that they will have online certifications that will demonstrate certain practices to keep their information safe. There will also be a system that sees if they are taking their certification courses by a certain deadline of the month. If they fail to meet their certification requirements that will lead to them being put on a probation period, and that could lead to termination of their current position. There will also be “fake” phishing emails sent to the employees to see if they have been paying attention to the courses and learning from them. If they fail to react accurately to the phishing emails, there will be consequences such as demotion or certain courses that will have to take in order to obtain status back in their current position. In addition to this, there will always be monthly briefings talking about the current issues of cyber security and what the company is doing to keep them from having breaches in them. With that being said, everybody in the company will be responsible for being up to date and current on cyber security issues and ways to keep themselves secure from getting their information stolen.