Risk Assessment System; Does It Help or Hurt?

So let's say that your employer is collecting a large amount of data on you and your fellow employees. This data is then shoved through some automated system to track the risk that said person is to the company. Those at high enough risk are extensively checked and put on watch to ensure that said people either don't defraud the company or if they do actions can be done so quickly to locate and handle the incident. Those at even higher risk are terminated instantly for being too risky. These insider threats could be anything from embezzlement, an employee's phone being compromised and spread it, or a hacker group giving one employee a thumb drive. This risk assessment system may seem understandable from a security person's perspective. We can minimize risk by getting rid of its from the source. However, to an employee who is shell shocked by the sudden collection and use of data on them, they may believe that they did not consent to these actions. Or it could seem like an invasion of privacy to a separate employee. Both of these very well could be considered valid complaints towards the system that was created. So let us look into how this automated risk assessment could be implemented improperly and the ramifications of the use of such a system.

A large potential issue that may happen with setting up and using such a system that collects and analyzes data on employees is that it may be seen as a violation of the personal privacy or rather the employee's expectation of privacy. Such an issue could even end up in court. However, according to "A Gift of Fire", the court's decision on a dispute of privacy between an employer and their employee often depends on the employee's reasonable expectation of privacy within the workplace and/or on corporate systems. This means that setting clear terms to explain the use of the system and why is needed. "A Gift of Fire" explains to do so within companies policy by ensuring it has clear statements that employees can understand. This ensures that employees learn why the system is being used and what data is being collected. That way they can comprehend the reasonable level of privacy within the company with regards to the automated system being used.

A second issue that could arise from this system regards getting the consent from the employees. From our reading over the RFID implant, "[obtaining an employee's] consent would most likely be a complete defense for the employer against any privacy claim". This makes it vital for employers to ensure that they obtain consent from their employee to allow the automated system to rank their risk. However, for a good basis to get consent ethically, the employer should follow the ideas of informed consent, which we talked about in class, so the main focus is that each employee understands what is being collected and how it will be used. As well, then the employee can withdraw from the risk assessment system at any time with no repercussions. Regarding withdrawals, this kind of breaks the purpose of the system but is necessary to ensure that an employer cannot enforce the use of the system on their employees. However, there are high security workplaces both in and out of the government that can enforce the use of this, otherwise it would be too high of a risk to let some be off the system. These places should still shoot for most of the informed consent principles.

An additional ethical consequence that arises with the use of this automated risk system occurs when firing people even if they haven't done anything wrong but are labeled as high risk employees. There is nothing to my knowledge that would make this illegal as for the most part employers have the freedom to hire and fire who they choose as long it doesn't violate the employee's contract or the company's policy. However, this abrupt firing becomes ethically shaky. Looking at this from a utilitarian perspective, the employer lays off the employee making them unemployed but lowers the risk of harm by an insider because one system said they aren't to be trusted. There's hardly a benefit in most cases for a life changing negative effect to the people who are fired. So is it really needed to fire those that are a high risk to the business? We could in fact deploy risk management training for those that seem to be high risk. However, that won't simply fix everything. For instance, wealth could play a factor in the risk one exudes. Lower income workers could be more susceptible to financial payments for plugging some flash drive into a server. Thus also making this automated system potentially being discriminatory against those that align to be high risk to the system.

I talked about how this system could unfairly lay off workers under the guise of risk and potential discriminate groups such as the lower income workers. These actions add all the more reason to the 1000 reasons to "turn" that we talked in lecture regarding insider threats. That means that the use of this risk assessment system could in turn generate more risk to the business by motivating people to attack the business when they were / are layed off or discriminated against. Another potential risk from the creation of this risk assessment system could be the effect it has socially within the business. This system effectively is a ranking of trustworthiness of all employees. Along with that it becomes obviously apparent when people aren't trustworthy and start to be investigated. Those people may start to be looked down upon and not trusted by their coworkers because of the automated system. This would ultimately hurt the business and make people feel segregated.