(499 out of 523)

Farid Rajabinia (Fr2md)

ICS (HW3)

Have we considered not only our own perspective, but the likely perspective of other stakeholders?

It is impossible to consider all stakeholders when implementing security procedures. A comprehensive security implementation is impossible in terms of any company's resources and costs. Therefore, each company has to prioritize the benefits and security of stakeholders directly involved with the company, including investors, users and clients. The national and public interests usually follow in the priority list. Consequently, it is hard to adequately reflect on ethical harms that may be done by a security breach.

As a company, it is a reasonable decision to put the interest of the company first. But it might not be an ethical choice when the public interests are involved. For example, if a company has the most effective solution for a malware disrupting the worldwide network, it is against the public benefit not to share the cure with everyone. It can easily save lots of public resources all over the world. However, the interests of company dictate to keep the solution for subscribed users and employees only.

The consequences of this example might be different in short versus long term. In the Short term, it might protect the benefits of the company, but at the same time there are so many other people who are suffering. Although it is the legal decision not to share the solution, it might not be ethical because it is against the greater good. It is the trolley problem, sacrificing 50 people to protect 3 people who pay for subscriptions. In the long term, however, the reputation of the company might get hurt since it sacrificed public well-being for the benefits of its own.

There is no single solution for all the problems regarding cyber security. The decision is highly dependent on each scenario "and the specific risks, benefits, tradeoffs, and stakeholder interests involved." The best decision might come after careful considerations of all facts and options. The decision must be followed by "well-reasoned ethical judgment." It is always an ethical challenge for security professionals to balance security with other values specially in terms of stakeholders' interests who are both directly and indirectly involved with the security implementations and the consequences of its failure.

Transparency and disclosure are important factors in cyber security directly affecting stakeholders. Whenever there are risks caused by the company that put the interests of other parties at risk without their knowledge, it is the ethical duty of the company to make the risks public in order to minimize the consequences. However, there is no clear-cut instructions regarding the appropriate way and the extent of this disclosure. It is very subjective to each situation. In the Equifax breach, the extent of the damage was known almost a year before its public disclosure. They could have saved future damages if it was acted upon immediately. However, the interests of the company and its shareholders got the first priority. They tried to delay its disclosure to avoid the ultimate blow from public. However, they sacrificed public wellbeing and the greater good for their own benefits.