# Ethical Hacker 2 – Law, Ethics and Responsible Disclosure

* **Find a few examples of cyber-crime cases (sentences and penalties). If you are a student from abroad, find such example cases from your home country.**

My home country, Romania, is among the last countries in Europe to adopt a cyber-security set of laws. Until now I was not aware of any sentence for this crime in my country and after rigorous research, I still did not manage to find anything. However, it is quite often that public Romanian institutions get attacked because of their low security. The most common cyber attacks against these institutions consist of obtaining passwords and leaking confidential data. Attackers from Romania and eastern Europe, especially from Russia take advantage of the poor security of our institutions’ IT systems and for now there are very little to no consequences for them.

* **Describe what you will do if you find a high risk vulnerability, unexpected, in a website or IT-infrastructure (after reading the** [**CVD policy**](https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline)**) Take into consideration if you want to make money or make the world a safer place.**

I would comply to the disclosure regulations, if applicable and would report the vulnerability found straightaway, no matter what the preconditions and the promises of the company may be. In my opinion it would not be worth the risk since there are countless other ways to make money.

* **Find two or three companies and explain the concept of responsible disclosure they have in place and compare those companies.**

1. Philips -> they put more emphasis on the reward and are very vocal when it comes to what the tester can and cannot do. Their reporting procedure is slightly more complicated in comparison to the other two companies.
2. Microsoft -> they are very specific when it comes to defining the risks and vulnerabilities found by the tester. They specify that no legal action would be taken against the tester, but no mention of a reward. They believe that the knowledge gained throughout this process is rewarding enough.
3. Carestream -> their reporting procedure is very simple and straightforward: one form the tester has to fill in. They specify that no legal action would be taken against the tester, and also a mention of a reward. They are very specific when it comes to what the tester should do and what the company should do throughout this process.

**The links:**

* Philips: https://www.philips.com/a-w/security/coordinated-vulnerability-disclosure.html
* Microsoft: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW5Alv
* Carestream: https://www.carestream.com/en/us/services-and-support/cybersecurity-and-privacy/coordinated-vulnerability-disclosure