12. Whistleblowers and Bug Bounties

COMP6441 • KC Notes

12.1 Whistleblowers

- **Information easily flows, and it is difficult to keep a secret**
- Employees may internally tell the outside world when they are not meant to, when a company is not doing good things
    - American elections – when a candidate is bad
    - In security, we should consider not just why and what, but the **consequences** of leaking information
- Whistleblowing is **usually against a powerful organisation**
    - There is usually a standard way whistleblowers are treated:
        - Companies attempt to distract the media by discrediting the whistleblower
        - They are targeted – know that powerful people will ruin your life.
- Australia does **not have good whistleblower protection**
    - Be a Snowden
    - Be very careful if you do share company secrets
    - Cover your tracks

12.2 Vulnerability Disclosure and Bug Bounties (Guest Speaker)

- Vendors **do not need to respond to vulnerabilities**
    - People who find vulnerabilities threaten to sell, share or disclose a bug
    - St. Jude pacemakers: researchers found they could remotely drain battery and administer shocks
    - Often involves not only security, but the financial sector
- **Don’t monetise security research you have already done**
    - If it ends up on a legal team, it may have consequences
    - Don’t do stupid things, like DOS
    - Be practical: do bug bounties
    - Find a balance for when you stop when you find a vulnerability
- Bug bounties are hard to get into now
    - Find a niche – for example, the speakers found their niche in crawling for new Amazon services or new sites that were new and not documented