



Public health services in a poor country illegally reproduce patented Western medicines to create an affordable generic drug. They risk potential litigation that could cost their country millions in legal fees.



A mining company is trying to extract gas on prime agricultural land. The local economy is struggling and desperately in need of jobs, but any mining activity risks permanently polluting the groundwater.



A phone company scans all text messages sent between its customers for evidence of illegal activities. Customers are unaware their messages are being read by the company but have previously signed the terms and conditions.



A major national bank has lied about their finances by changing key data to inflate their share price deceiving investors. A scandal could cause the share price to crash and destroy many retirement pensions nationwide.



A major global search engine has been heavily criticised for changing its algorithm to 'unfairly' prioritise its products and services over other competitors. Some reviews have misled customers with tragic consequences.



A website is refusing to decrypt consumer data to the authorities citing privacy concerns, despite a request from police as the suspect is a known murderer. Such information would mean other users' data would be compromised.



A game developer will soon release a new game that retails for CNY¥480. They plan to limit access to online multiplayer by requiring players to pay an extra ¥50 / month. Better equipment and abilities will require additional payment.



An old public school that only admits the best and brightest is considering admitting below average students in return for “donations”. The money will be spent upgrading old facilities, buying new textbooks and hiring more teachers.



Unvaccinated staff at a public hospital have been told to get the vaccine or lose their job affecting 20% of the staff. The government is insistent, stating that medical workers must set an example for the entire community.



A large weapons company on the brink of financial collapse and employing over 50K locals has developed a deadly new weapon. Several governments have shown interest but many will likely use the weapon against their own civilians.



An energy company wants to use nuclear energy to reduce emissions. Locals are worried the plant will hurt the environment. Wind and solar are also being considered but won't generate enough energy to meet future demand.



A struggling national fashion label has begun outsourcing production overseas to cut costs. Local workers recently made redundant are outraged saying the company has betrayed the country and the community.

functionality
/fʌŋkʃən'æliːti/

reverse engineer
/rɪ'vɜ:s ɛndʒɪ'nɪə/

hack
/hak/

espionage
/ɛspɪə,nɑ:ʒ/

generic
/dʒɪ'nɛrɪk/

patented
/'peɪtəntɪd/

litigation

/ˌlɪtɪˈɡeɪʃən/

inflate

/ɪnˈfleɪt/

deceiving

/dɪˈsiːvɪŋ/

algorithm

/ˈælgərɪðm/

encrypt

/ɪnˈkript/

compromised

/ˈkɒmprəmaɪzd/

The website went down last night but full **functionality** was restored before the end of the day.

If we take it apart and look inside, we might be able to **reverse-engineer** it and copy the design.

If you have good cyber security practices, it'll be harder for criminals to **hack** your servers and steal data.

Expect all companies to conduct **espionage**. Keep data safe and secure. Trust nobody.

The **generic** was much cheaper than the brand-name painkillers and just as effective.

The company has hundreds of **patented** products and designs with more pending.

Be ready for **litigation** by angry customers and upset employees who may take legal action.

Despite **inflated** expectations, investors were left disappointed by the share price this week.

Deceiving your friends and family isn't a good idea because they'll never trust you again.

Online media is driven by an **algorithm** that decides what we see and hear.

If you properly **encrypt** your data, it's nearly impossible for bad people to read or use it.

If you share your password with others, your data and finances may be **compromised**.

Tau Electronics Chief Operating Officer

Your company was responsible for the cyber-attack on Switch Electronics. The data you've managed to get will help your company fast-track development of critical telecommunications equipment for deployment in poor and rural areas of Africa and Asia.

Tau Electronics prides itself as a major local employer and driver of innovation and change. You feel conflicted about what has transpired, but don't know what to do as the operation was approved by the CEO herself.

Switch Electronics Junior Engineer

You were responsible for the disappearance of Switch Electronics' prototype phone. You accidentally took it home last night after work, but nobody knows you have it, nor do they know you had access to it.

You're overworked and underpaid and could sell it for a high price to another company. If you tell your boss what happened, you risk losing your job and will likely be blacklisted by your company making it hard to find future employment.

Boss: Good morning. I'm afraid I have some bad news. One of our senior engineers has reported that a prototype model of our new phone has gone missing and is suspected stolen. Whilst the design wasn't complete, ergonomically speaking, it did have full technical functionality. Additionally, we've had word from our security specialists in IT that we've been victim to a hacking attempt. An external party was able to bypass our firewall for several hours last night, and our servers - containing various design and R&D documents - have been accessed. It seems we've suffered an act of industrial espionage. We urgently need to assess how damaging this could be to us.

Manager 1: Well, the latest technical documents aren't stored on the servers, they're on machines with a full 'air gap'. So perhaps it's not a total disaster.

Manager 2: But if they have the prototype phone, our counterparts at whichever rival did this will soon reverse engineer the technology. How about intellectual property laws? Are any of these designs patented yet? And do we have any idea who has been spying on us?

Boss: We strongly suspect that we were hacked by a company called Tau Electronics, a major player in the Asian mobile phone and tablet market. Unfortunately, IP isn't recognized in the country where the hacking attempt originated. If they modify our designs, it will be very difficult to prove that they stole the tech from us. We need to decide our next steps ASAP. Any ideas?

Manager 1: Well, it's a race to the finish line now. We have to make sure our product comes out before theirs. And maybe we can get the marketing department to include some tech-specs in their ad campaign - to stay ahead of the game.

Manager 2: Agreed, and we need to review our cyber-security and counter-espionage procedures. We can't allow our hard work to fall so easily into the hands of the competition.

Boss: OK then. I'll organize a separate meeting with marketing and arrange for a full security review. Thank you both for your time. Let's get back to it...