COSC 244
Haoyang Gao
3970509

Ethics

Jill may feel bad when read the following sections in the report:

The best way to check would be to count the ballots by hand, or examine any paper or electronic trail available in a thorough and public audit. This is not happening. So the short answer to this question is: We wouldn't know if the totals were wrong. Or would we?

And yes, she may feel even more bad when find out that her company may become the malware source installation place.

It means that she has found some security risk which may harm the core business of her company, and furthermore, a huge impact to the clients. She needs to take some action and it is good to know that there are already some guidelines for her to follow:

1. Have a good faith to her colleagues. Don't suspect anyone or invent some kind of conspiracy theory. This is to obey the IITP Code of ethics (1) Good faith.
2. She needs to inform the company and the clients about the fact that she discovered. This is to follow the IITP Code of ethics (3) Community-focus. And the IITP Code of practice 2.9 point 4:

   > *Seek to identify potential hazards, failures and risks associated with your work or work place, and seek to ensure that they are appropriately addressed.*

3. Check the work that she leads to reduce the risk as best as she could. This is to obey the IITP Code of practice 2.9 point 5:

   > *Ensure that those working under your supervision or direction are competent, that they are made aware of their responsibilities and they accept personal responsibility for the work delegated to them.*

   And this process should inform the company and the clients as well.

Johan encounters such a dilemma which the personal interest of his company and him may related to some risky move. And the risky may not be burst at first, but when it does, the result will be very nasty. So it may look like very tempting.

But the math is simple, any bad news in the future will connect to his company and him, such short-sighted behavior will destroy his company and his own career path. Even there is not, the potential risk out there which may influence the public voting outcome will blame his conscience daily.

Since the context mentioned that Johan is an expert, so I consider that Johan knows all the pros and cons. What he should do is as the following:

1. He should elaborate the pros and cons thoroughly. And suggests 'not to take part in such action.' This is as the IITP Code of Practice 5.1.1 point 8 said:

   > *Demonstrate an understanding of the business issues; be persuasive and explain to users and management, in language they understand, the benefits of the changes being introduced, as well as identifying any drawbacks and trade-offs.*

   And for the IITP Code of Practice 3.3.2 point 3 as well:

   > *Ensure that the decision-makers are fully aware of all the relevant facts and the possible consequences of their decisions.*

2. Since the context mentioned the regional council, I consider the impact will be huge (affect a wide range of places). He should consult with all stakeholder groups. This is to obey the IITP Code of Practice 5.1.1 point 3:

   > *Involve and consult representatives of all stakeholder groups.*

3. If any pressure faced, obey the IITP code of practice 3.3.2 point 2:

   > *Resist any pressure to oversimplify the risk analysis; involve personnel at all levels within the organization to elicit the threats and the vulnerabilities to those threats.*

The section of IITP 3.5.1 When advising on Business change can also be adopted as well:

> *Point 3 : Challenge any apparent malpractices and investigate the root causes.*
>
> *Point 7 : Show sensitivity to political and cultural issues as well as technical and business effectiveness targets.*

Irinushka's situation is a little bit complicated since now her client is the government rather than some normal companies or individuals. The context is the domestic media in her country has formed the different portraits for two American leaders. Then the government has approached her to do something.

What she need do is just one thing, and one thing only.

Just 'NO'. No matter which one is more evil or not, no matter the local media has tried to brainwash the people or not. The behavior itself is wrong regardless of any appearance the government wants to decorate.

I am very happy that IITP Code of ethics is with me all the time as well as this one.

> *IT Professionals will practice with: Integrity - Members shall act in the execution on of their profession with integrity, dignity and honors to merit the trust of the community and the profession, and apply honesty, skill, judgement and initiative to contribute positively to the well-being of society.*

Manuel surely has some professional under his belt. And the time is just that right. There is not any bad consequence yet. What he should do is obvious:

1. Don't try to fix it. Even suddenly a so-called inspiration hits you. As the IITP Code of Practice 5.6.4 When Investigating Problems Point 6 says:

   Appreciate the consequences of making changes to operational systems: resist the temptation to make ad hoc fixes unless you are certain they will work.

2. Let your leader know this issue as soon as possible. The IITP Code of practice 5.6.4 When Investigating Problems Point 7 supports on this too:

   Bring to the attention of your next level of management any problem that you are unable to resolve within the target timescales.

3. And should strongly suggest that this machine should be abandoned immediately, should use the backup plan such like "hand-counting". There is no political and social chaos if you point out this issue. There will be a huge issue if you try to hide it. As the IITP Code of ethics says:

   Community-focus - Members' responsibility for the welfare and rights of the community shall come before their responsibility to their profession, sectional or private interests or to other members;

4. Don't afraid of the threat. The IITP code of practice 3.3.2 point 2 says:

   Resist any pressure to oversimplify the risk analysis; involve personnel at all levels within the organization to elicit the threats and the vulnerabilities to those threats.