

Assignment 06

Name	Juan Callejas
Career field	Economics
Country	Guatemala
ESG Topic	Data privacy and cybersecurity

You may continue with the assigned topic in Assignment 05 or choose another one. The topic you select for Assignment 06 is your ESG Topic for your capstone project. For a range of topic possibilities, see Week_06_Hayek-Ferrarini_PPT (2013: Slide 36).

Instructions:

1. Guatemala macro indicators¹
 - a. GDP: US\$85.99 billion²
 - b. GDP annual growth rate (2022): 3.5%
 - c. GDP per Capita: US\$4,388.44³
 - d. Inflation: 8.32%
 - e. Interest rate: 5%
 - f. Corporate tax rate: 25%
 - g. Personal income tax rate: 7%
 - h. Internet access in Guatemala⁴
 - i. 62% of the population has access to a cell phone.
 - ii. 91% of all internet users in Guatemala access the web through a cell phone.
 - iii. 92% of all cell phones in Guatemala are used through pre-paid plans.
 - iv. As of 2018, 29% of Guatemala's total population has access to the internet.
 1. 21% of the population has a computer at home.
 2. 17% of the population has access to a home internet service.
2. Data privacy and cybersecurity
 - a. ESG issue:
 - i. According to the World Economic Forum⁵, cybersecurity should be regarded an ESG issue for three main reasons:

¹ (n.d.). *Guatemala Indicators*. Trading Economics. Retrieved May 27, 2023, from <https://tradingeconomics.com/guatemala/indicators>

² (n.d.). *Guatemala Indicators*. Trading Economics. Retrieved May 27, 2023, from <https://tradingeconomics.com/guatemala/gdp>

³ (n.d.). *Guatemala Indicators*. Trading Economics. Retrieved May 27, 2023, from <https://tradingeconomics.com/guatemala/gdp>

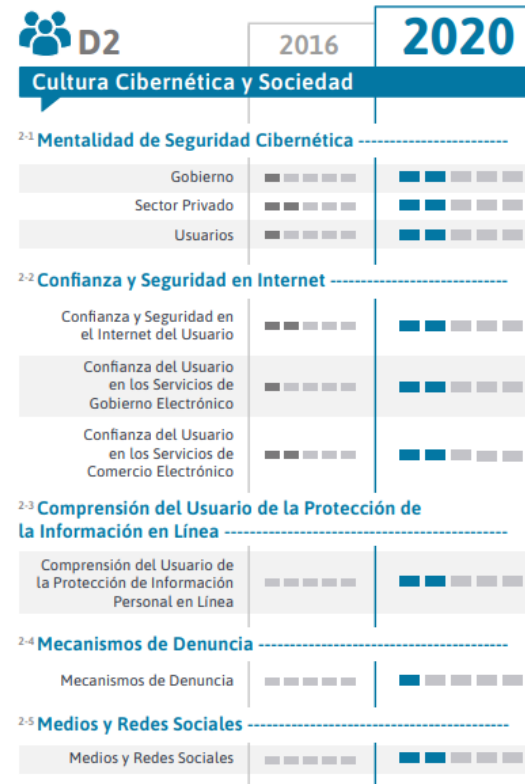
⁴ Instituto para la Competitividad Económica (2022, June 6). *¿Cuál es la penetración de internet en Guatemala?* Retrieved May 27, 2023, from <https://iceguate.org.gt/cual-es-la-penetracion-del-internet-en-guatemala/>

⁵ Instituto para la Competitividad Económica (2022, March 1). *Cybersecurity is an environmental, social and governance issue. Here's why*. World Economic Forum. Retrieved May 27, 2023, from https://www.weforum.org/agenda/2022/03/three-reasons-why-cybersecurity-is-a-critical-component-of-esg/?DAG=3&gclid=CjwKCAjw1MajBhAcEiwAagW9MUgEjYRtBTDKGqNsXC1HtMmlhJaiiI2hg-jLRpz-hM4jkwYJJvdJBoC0yIQAvD_BwE

1. It presents a threat to value.
 2. It presents a threat to society.
 3. Insurance can't mitigate the risk indefinitely.
- b. Cybersecurity in Guatemala
- i. Cybersecurity has been a growing concern in Guatemala over the past few years. Many private companies⁶ are offering comprehensive cybersecurity solutions for companies, and colleges are offering cybersecurity graduate degrees⁷.
 - ii. Since 2018, the [National Cybersecurity Institute](#) was created to raise awareness, train, and develop a stronger cybersecurity culture in the country, and partner with companies, universities, and the government in strengthening our national infrastructure for this. The institute partners with the government's [National Science and Technology Secretary](#) to further its efforts as a member of the [Intersectoral IT Technical Commission](#).
 - iii. [Awareness has grown in Guatemala as improvements across the board of key indexes proves over the past years:](#)

⁶ (n.d.). *MEJORES EMPRESAS DE CIBERSEGURIDAD EN GUATEMALA*. For Guatemala Lovers. Retrieved May 27, 2023, from <https://www.forguatemalalovers.com/es/mejores/empresas-de-ciberseguridad-en-guatemala>

⁷ [Universidad Internaciones](#) and [Universidad Galileo](#) offer master's degrees in Cybersecurity





This shows that a comprehensive approach involving academia, business, communication, culture, and government (legal, judicial, public policy, etc) has been fruitful and although the improvements are small, they continue to grow.

3. Solutions

a. 100% Government

- i. Government mandated cybersecurity standards through legislation and regulations for all businesses.

- ii. Price fixing of minimum requirements to pass cybersecurity standards assessments.
 - iii. Legal, judicial, and penal code reforms to investigate, pursue, judge, and punish cybercrime.
 - iv. Adopt international standards like [HIPAA](#) to enforce data privacy regulations and standards in the country.
 - b. 100% Market
 - i. Companies understand, through training and organizations like [INCIBEGT](#) who raise awareness, their need to adopt cybersecurity measures to protect their information as well as their customers.
 - ii. Companies contract solutions from international providers.
 - iii. Academia understands the need and begins offering education and certification.
 - iv. Local cybersecurity companies begin to appear and offer competitive solutions and prices.
 - v. Local private entities, such as INCIBEGT, begin to develop shared standards and consensus around important cybersecurity frameworks to better protect companies and end users. These entities help draft basic legal frameworks to investigate, pursue and punish cybercrime.
 - vi. Companies and end users are held 100% accountable for the consequences of improper use of IT technologies, cybercrime, and privacy breaches.
 - vii. Companies begin to demand from suppliers basic cybersecurity standards in order to do business with them.
 - c. Corporations seeking to satisfy shareholders and stakeholders.
 - i. This approach would look very similar to the market approach although a major difference might be stronger lobbying from “cybersecurity guilds” to block foreign entrants, require certain legal licenses to offer services and to legally require companies to abide by standards that are way beyond their needs and might make them less competitive.
 - ii. Corporations might also promote the blocking of specific legislation and regulations that protect individual data privacy so that they can exploit it, sell it or use it for marketing purposes.
- 4. Discuss the advantages and disadvantages of each approach and include opportunity costs.
 - a. Government
 - i. Advantages
 1. Centralized control of policy, regulation, and standards.
 2. Price fixing can allow smaller companies to afford solutions.
 - ii. Disadvantages
 1. Minimum standards can disincentivize companies from adopting stronger measures to protect their information and their customers.
 2. More qualified solution suppliers can withdraw given price caps.
 3. Corporations can lobby for looser legislation and regulation for their practices.
 4. Corporations can also lobby for licenses for new entrants in the cybersecurity solutions space in order to protect local industry.

5. Legislation and regulation can easily fall behind compared to the rapid advances in technology.

b. Market

i. Advantages

1. Competition promotes innovation around the cybersecurity space.
2. Companies assume responsibility and are accountable by the market for how they protect their information and their customers'.
3. New businesses and new academic tracks for IT professionals can develop around the cybersecurity space.
4. Companies can choose from a variety of solutions to set up in their business and customers are more empowered to choose whether to share private information and whether to authorize companies to use it.

ii. Disadvantages

1. No minimum, legally mandated standards.
2. Customers might not have legal recourse when privacy is violated.
3. With no standards or regulation, fake businesses can be set up that cheat companies and users by selling bogus cybersecurity solutions.

c. Corporate

i. Advantages

1. Corporate consensus around standards allows for better protection of private or sensitive information.
2. Corporate pressure can help prosecute cybercrime.
3. Corporate pressure can motivate more companies to adopt cybersecurity measures and standards.

ii. Disadvantages

1. Corporations can lobby and promote legislation and regulation that benefits them, and leaves end users unprotected.
2. Corporations can lobby for licenses that prevent new entrants from competing in the market.
3. Corporations have more resources to defend themselves from lawsuits and through LLC regulation, avoid personal responsibility and accountability for cybercrime.

5. Take an informed stance with a rationale.

- a. I will always advocate for a market approach to the cybersecurity issue, with a basic legal framework that gives recourse to the investigation, pursuit and prosecution of cybercrime and data privacy violations.
- b. It is important to foster private efforts to educate the population, and form new, well trained cybersecurity professionals that can build new companies that offer a wider array of options and solutions.
- c. It makes sense that the government invests in training police, prosecutors, and judges in understanding cybercrime in order to better engage these issues as they arise.
- d. Private NGO's like INCIBEGT are key to form a stronger cybersecurity culture in the country that helps protect businesses and individuals.

Assignment 05

Name _____

Career field _____

Country _____

Instructions: Use critical thinking, data, and academic articles to present two extreme solutions to addressing your assigned issue. One solution should be a market response, and the other should be the government response. Identify the advantages and disadvantages of each approach. Conclude with an informed stance, and provide a full list of properly cited sources. (Use your favorite browser to find a citation machine. Use your industry's standards for proper citation format.)

Ethical Business Practices (Last names begin with A-D)

Managers might engage in unethical behavior such as bribery, corruption, or fraud, which can have severe negative impacts on stakeholders and society. This can be motivated by personal gain or pressure to meet financial targets, disregarding the long-term reputation and sustainability of the company.

Governance and Board Independence (Last names begin with F-M)

Managers may resist or manipulate efforts to improve governance practices, such as the composition of the board of directors or the establishment of independent oversight committees. This can hinder transparency, accountability, and effective decision-making within the company.

Stakeholder Engagement (Last names begin with N-Z)

Managers might fail to adequately consider and engage with stakeholders beyond shareholders, such as employees, customers, communities, and the environment. This can lead to decisions that prioritize short-term financial gains while ignoring the broader social and environmental impacts of the company's operations.

With the help of Commercial Society (2020), do the following in your assigned area.

1. Analyze the role of trust, agency, and bystanders in a business situation connected to your assigned topic.
2. Evaluate the consequences of having or not having each concept in these situations, and identify strategies for promoting trust, empowering agency, and facilitating intervention on behalf of the bystander in your assigned situation.
3. Identify the advantages and disadvantages of the effectiveness associated with (i) government determined and (ii) market-based solutions. Next week, prepare to take the corporate possibilities.
4. Propose an integrated solution to promote trust, empower agency, and facilitate bystander intervention in a range of settings.