CLASS ACTIVITY: COLONIAL PIPELINE ATTACK

In this interactive activity, we analyze a scenario that is rich in cybersecurity ethics issues. Our main goal today is to answer the question: *What is the best (i.e., the most ethical) solution to the problem(s) identified in this situation?*

To answer this question, we engage in a **stakeholder analysis**. Here are the questions we will tackle:

1. What **technical issues** are present in the scenario?
2. What **cybersecurity issues** are present in the scenario?
3. Who are the **stakeholders** in the scenario (i.e., which people and organizations are affected)? What things that are valuable to them are at stake?
4. Who is **morally accountable**?
5. What is an appropriate solution? Consider several solutions that seem to be both the **most just** and the **most practical**.

**Let’s begin!** Form groups of three people, and give each person one of the following roles (or your instructor may assign groups/roles):

- A **facilitator**, who asks the first question and keeps the group moving forward with the discussion.
- A **quality controller**, who interjects questions throughout the discussion and ensures that everyone’s input has been received and that discussions and differences are handled in a principled way.
- A **recorder/reporter**, who records group responses and responds to questions from outside the group.
THE SCENARIO

Source: The Colonial Pipeline Ransomware Attack: Everything We Know by Gianna on May 19, 2021

What happened:
Throughout the week of May 10, 2021, headlines focused on the impact of a ransomware attack on the Colonial Pipelines and gas delivery across the eastern and southeastern United States.

People rushed to purchase gas which created greater shortages and resulted in many stations running out. There were long lines at many other stations.

As ransomware continues to plague public and private organizations, taking a deep dive into the Colonial Pipeline ransomware attack provides insight into how these attacks work.

How it Happened: How the DarkSide Ransomware Works

Stage One - Initial compromise stage where attackers gain access to a device, masquerading as a legitimate user so that they can install the malicious code on the compromised endpoint. Research indicates that cybercriminals do this in three ways:

1. Brute force password attack
2. Phishing attacks with malicious links
3. CVE-2021-20016, a SQL-injection vulnerability against an organization’s Virtual Private Network (VPN) infrastructure

Stage Two - Escalate privileges to gain access to sensitive information. Finally, they encrypt business-critical processes, request a ransom, show “proof of life” over the exfiltrated data, and decrypt everything only after the target pays them.
**Timeline:**
A Timeline of the Colonial Pipeline Attack

- ✔ May 6, 2021: Malicious actors launch an attack, stealing data, locking computers, and requesting a ransom.
- ✔ May 7, 2021: Colonial Pipeline pays the ransom.
- ✔ May 8, 2021: Colonial Pipeline publicly announces attack, then shuts off servers and some pipelines.
- ✔ May 9, 2021: Colonial Pipeline makes a second public announcement, discussing its system restart plans.
- ✔ May 10, 2021: The FBI confirms DarkSide ransomware caused the attack, and Colonial Pipeline releases two more statements around its restoration process.
- ✔ May 11, 2021: Federal agencies release an advisory describing DarkSide ransomware and mitigation strategies while Colonial Pipelines releases a statement around fuel shipping.
- ✔ May 12, 2021: Colonial Pipeline restores operations and announces fuel delivery timelines, amidst people “panic buying” gasoline.

**Why it Happened.**
A review of the timeline gives insight into the longer-term impact that a single, well-targeted attack can have on a system, infrastructure, region and even country. This high-profile case study demonstrates how a successful critical infrastructure Ransomware attack can have a devastating social and economic impact. In less than six days, an entire region of the US fuel supply turned precarious.

DarkSide is a type of Ransomware-as-a-Service (RaaS), not a group of attackers. According to the joint Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) release, the RaaS developers receive a share of proceeds whenever a cybercriminal group deploys it.

The "DarkSide actors/group" are considered cybercriminals deploying the ransomware and targeting organizations through phishing attacks or exploiting user accounts, systems, virtual machines, servers and cloud infrastructures. Although the first instance of DarkSide ransomware appears to have been in November 2020, research indicates that threat actors deploying DarkSide have signatures that can be traced back to April 2019. Additionally, those early attacks indicate an inactive period existed between the initial compromise and the ransomware deployment period.
Fake Communication

Source: https://www.phishing.org/phishing-examples
Ransom Email

WHAT ARE THE ISSUES?

Each question is designed for an individual or group response. Respond accordingly.

1. **Individual response:** Summarize what happened in 2-3 sentences.

2. **Group response:** Email systems are popular targets of hackers. Provide three reasons why.
   
   a.
   
   b.
   
   c.
3. **Group response:** Let’s place what went wrong into three different categories. Provide a few examples of each below:
   a. Technical
   b. Process
   c. Human error/poor judgment

### WHO ARE THE STAKEHOLDERS?

Here is a partial list of people and organizations that were impacted by this event. In ethics terminology, we refer to them as *stakeholders* because they hold values at stake because of the scenario’s events:

1. Users, Technology and Security Staff
2. Technology, Security and Operations Managers
3. Executives and Stockholders
4. Law Enforcement
5. General Public
6. U.S. government and other governments
7. Hackers

4. **Group response:** Divide the stakeholders listed above among your team members (two per person): Identify what’s at stake for each stakeholder in this scenario. This can be *anything of value* to people or communities in that category.

1. Users, Technology and Security Staff
2. Technology, Security and Operations Managers
3. Executives and Stockholders
4. Law Enforcement
5. General Public
6. U.S. government and other governments
7. Hackers
5. **Group response:** What did each category of stakeholder do to contribute to the problem? This is referred to as *accountability*.

- Users, Technology and Security Staff, Technology, Security and Operations Managers
- Executives and Stockholders
- General Public
- U.S. government, other governments
- Hackers

**HOW CAN WE PREVENT THIS KIND OF PROBLEM IN THE FUTURE?**

Based on your analysis so far, consider the technical problems that led to the event, the people and organizations that were affected by it, and the actions and degree of accountability that you assigned to each group of stakeholders. Now it is time to suggest a remedy, so that this kind of thing does not happen again!

6. **Individual response:** Provide a policy that you believe would be effective and would deliver the greatest degree of justice. Think about *all* the stakeholder identifications and the issues of accountability that you came up with in the previous section. How does your policy hold the appropriate parties accountable? How does it address the values at stake?

7. **Group response:** Compare your individual policies. Craft a consensus policy proposal among your group. It should be both practical and **just**. Justify your choices! Again, consider the stakeholders and their accountability.

**INDIVIDUAL REFLECTION**

**Individual response:** Describe what you have learned from this scenario about the social and ethical impact of cybersecurity risks and breaches. Also, describe what you have learned about the relationship between privacy and cybersecurity.
HOMEWORK QUESTIONS

1. Based on your responses to Question 3 on page 6, how would you characterize the attitudes toward security taken by key players involved in the scenario?

2. On page 6 we identify seven categories of stakeholders. Identify one more category of stakeholder, describe what values are at stake, and assign the degree of accountability you think they deserve. Justify your answer.

3. Review your group’s final proposal from Question 7. Briefly describe what you might change now that you have had some time to think about it.