# SY403 – Second Short Exercise (10 September 2019)

The cybersecurity exercise you will build on Short Exercise One's introduction of an analytical discipline known as "serious discovery gaming."  As before, this particular serious game will employ a cybersecurity vignette, with the goal of gaining insight into the:

- Key issue(s) and their root causes
- Primary stakeholders, their equities, and the relationships between them
- Possible solutions and their associated costs, incentives, and impediments

**Before Class:**

Read the Detroit Free Press article about the ransomware attack  - **beginning on page 2 of this document.**

**In-Class Instructions for the Ransomware Exercise**

The White House is convening the following stakeholders to discuss plans to minimize further harm in Detroit, and to prevent other U.S. organizations from becoming ransomware victims:

- City of Detroit
- Business Software Alliance (organization representing the world's largest software makers)
- National  League of Cities
- Federal Bureau of Investigation
- National Security Agency
- Department of Homeland Security
- Office of the Secretary of Defense
- State Department

You will be assigned to small groups of 2-3, with each group representing one of the stakeholders. You will have about 30 minutes to develop a proposed strategy, both for Detroit and the nation. Each group will briefly present its strategy, and then attempt to negotiate a consensus approach.

As in exercise 1, the success of the game (and value you derive from it) will be directly proportional to your personal engagement.

**Background Reading (Scenario) for SY403 In class Exercise, 10 September 2019**

**Detroit Free Press**

November 1, 2019

The city of Detroit remains paralyzed for a fourth day, after a ransomware attack effectively shut down most city services. Economists predict that the attack is costing the city and private sector millions of dollars each day, but the city has shown no signs of willingness to pay the $250,000 demanded by the hackers.

"Detroiters don't back down," Mayor Mike Smith said. "We are making it abundantly clear to the world that we will not cave to extortion or threats."

The impacts of the ransomware have been dramatic and crippling for the city and its residents. Smith told reporters at a news conference that the city's garbage collection would be suspended for at least another week. This has caused trash to collect on the streets, and many local businesses, such as restaurants, have been unable to operate. The city police continue to show up for work, but without access to computers their work is effectively halted to a crawl. The Detroit Public School system will be shut for the foreseeable future. Because more than half of the city-owned electric utility is non-operational, Detroit-based manufacturers have halted production and furloughed employees.

Smith won election in 2016 on a "Detroit 2030" initiative, which promised to shift all city services to a centralized platform by 2030. He had complained that even in 2016, much of the city's business had been conducted via paper records, and that the city had hundreds of different computer systems, many of which ran Windows 95.

He has mostly made good on his promise, shifting garbage collection, public schools, public works, emergency services, and municipal administration to a centralized computer system operated by a private company, ComputerInc. ComputerInc is a 50-employee company that has never built a system as large as what Detroit requested, and has little experience with cybersecurity. However, the CEO, John Jones, is Smith's brother-in-law.

According to a response to a FOIA request filed by the Free Press for information about the $1 billion, 10-year project, the contract imposes no requirements for cybersecurity safeguards. This is a significant deviation from common city contracting practices, even for smaller projects that involve far less sensitive data and systems.

It is unclear what, if any, cybersecurity safeguards ComputerInc has adopted. Jones slammed the door in the face of a Free Press reporter who confronted him at home. A city employee, choosing to remain anonymous, told the Free Press that the default password to his agency's ComputerInc-connected system is "password," the system does not support multifactor authentication, employees do not receive cybersecurity training, and all agencies that have migrated to the centralized system have full access to the other agencies' files. "I'm just a line worker, but it says that I have 'administrative rights,'" he said. "What does that mean?"

At the press conference, Mayor Smith acknowledged that the city of Detroit does not have any local or remote backups. "ComputerInc assured us that its systems were 100 percent secure, and we had no reason to doubt them," Smith said.

The lack of cybersecurity safeguards was a critical component of the attack's success. According to a source within the intelligence community, the attack has been traced to a crime syndicate in Russia, which makes tens of millions of dollars each year by targeting ransomware at municipalities and large corporations. Although the organization is non-governmental, the Russian government knows about the organization and has informed its leaders that the government condones the acts and will protect the organization from prosecution.

Detroit is one of a dozen major U.S. cities to suffer ransomware attacks in the past month. Detroit is unique, however, because it is the only one of the cities to refuse to pay the ransomware. Of the other cities that have paid ransomware demands, eight were able to immediately recover all of their data and operations within a day, while three were unable to restore most of their data and have had to rebuild their affected systems. Detroit also is unique because it is the only city that has no segmentation between departments, allowing a single ransomware infection to quickly spread across all city systems.

The intelligence community source stated that there is substantial evidence that the crime syndicate is perfecting its techniques and targeting dozens of other cities in the United States, Canada, and Europe.

Detroit's systems were particularly insecure, the intelligence community source said, making them quite vulnerable to ransomware. But the crime syndicate's newest tools are far more effective, the source said, and have penetrated even the systems of organizations that have adopted industry-standard cybersecurity safeguards.

The intelligence community source would not comment as to whether the ransomware relies on any vulnerabilities that are known to the intelligence community but not the general public. "If the federal government knows about a vulnerability that allows the ransomware to spread, it has a duty to disclose it immediately," said Jane Johnson, president of the National League of Cities, which represents municipalities nationwide.

With the twenty-third largest city in the United States virtually shut down, the White House has called a meeting tomorrow with key stakeholders from the federal government, city of Detroit, and private sector, to develop a plan to help Detroit recover and prevent future incidents nationwide.