IN ASSOCIATION WITH

MODEL ANSWER C

CAPSTONE: CASE STUDY ESSAY

Assess the likelihood of an Iranian-backed cyber security threat to the water supply in Riyadh, and develop a plan for the Ministry of Interior that

- **responds to this threat by covering prevention, mitigation and response,**
- **utilizes international best practices, and**
- **is consistent with the ethical and legal responsibilities of security officers.**

Definition

Open Source Intelligence shows that Riyadh is a large metropolitan city with over 7 million residents. (Macrotrends, 2019). The city is supplied with water through two main sources:

1. Treated underground water, and
2. Desalinated water that is pumped via pipelines from 2 main desalination plants located at the Arabian Gulf.

Due to its large population and hot climate, Riyadh uses 3.15 million cubic metres of water a day (Argaam, 2018), with approximately one day's worth kept in emergency storage tanks (Ratcliffe, 2019).

So far there have not been any reported Iranian cyber-attacks on water-related infrastructure (Baezner, 2019; Paganini, 2020). A PWC report stated that businesses in the Middle East are more vulnerable to cyber-attacks than other places, with 85 percent of respondents to a survey claiming they were victims of an attack (Witt, 2020). Additionally, there have been at least eight attacks on Saudi Arabian assets by Iran since 2012. Even

though those attacks were not on water-related facilities, the fact that Iran used drones to target two Saudi oil refineries in 2019 (BBC, 2019) shows an escalation in hostilities and suggests a high probability of an imminent attack, thus warranting a review of threat assessments and security policies.

After establishing the likelihood of a threat, we need to identify the most likely target. As previously described, the water supply of Riyadh consists of water treatment and storage plants (shown in Figure 1), the pipeline distribution network, and two desalination plants located on the Arabian Gulf. Of those the locations, the most vulnerable to cyber-attacks are the water treatment and storage plants located in Riyadh and the desalination plants located at the coast. An attack on the desalination plant at Jubail would be especially devastating as it would force Riyadh to evacuate "within a week," as the plant provides over 90% of the city's drinking water (Jones et al, 2019). The same report (by Jones et al, 2019) has noted that "every desalination plant built is a hostage to fortune; they are easily sabotaged".

Figure 1: Location of Water Treatment and Storage Plants in Riyadh (shown as blue dots)

The threat assessment suggests that an attack on the water supply of Riyadh would have devastating consequence and is likely given Iran's recent aggression. A limitation of our analysis of the threat is that it is based entirely on backward looking data; we have not

seen any forecasts or predictions of Iranian activity in the region that would let us know whether to expect higher or lower levels of intervention. In addition, there is no historical data on actual cyber-attacks on water-related facilities; the assessments of likelihood and magnitude cannot therefore be benchmarked against actual incidents. Widening research to include non-Saudi cases could help provide analogous benchmarks.

As a consequence of the question, we assumed that the incoming threat is a cyber-attack. This made us dismiss pipelines as a likely site of attack. If, on the other hand, Iran uses drones to target the water supply like they targeted the oil refineries in 2019, this would change our working parameters significantly. It is highly recommended that a separate investigation team is assigned to assess the likelihood of physical threats to the water supply of Riyadh.

Innovation

The plan proposal consists of three parts: Prevention, Mitigation and Response.

Prevention

The first part of any plan is to prevent the attack from happening.

To do this, the first step should be to hire a cybersecurity consulting firm (such as Flashpoint, FireEye or IBM). The firm must carry out a full review of current cyber security practices at desalination plants as well as the as well as at water treatment and storage facilities. The consulting firm will be tasked with updating all cyber security software and firewalls with ones that meet industry standards wherever necessary. This will increase the security of the facilities against brute force hacks from the outside.

Another common way for cyber-attack to start is with phishing attempts to steal passwords and other access methods to the relevant computer systems. To prevent this, the consulting firm will need to create and deliver a rigorous education and training program that would be mandatory for all relevant personal (people who have access to accounts that can compromise the security of the facility) at the desalination plants and water treatment and storage facilities. Such training should be done regularly in order to refresh and update knowledge with the most up to date best practice. Personnel should also be discouraged from using the work computers for personal use, and their

computers should be routinely checked by the IT department in order to ensure that no breaches have occurred.

Mitigation

The second part of the plan will discuss possible ways to reduce the severity of an attack if one were to happen.

A big issue that Riyadh faces is its high-water consumption as well as low storage capacity. Currently there is only 2.87 million cubic meters of water stored for emergencies (Ratcliffe, V, 2019) within Riyadh's storage facilities. At the current consumption rate of 3.15 million cubic metres of water per day (Argaam, 2018), this will only be enough to provide water to the city for one day. If a cyber-attack were to happen that cripples all or most incoming water in the city. the Ministry will have a hard time putting a response effort in such a short timeframe. In order to mitigate this, the Ministry should build more storage facilities that will increase the water storage capacity to at least a week. The extra storage will add additional redundancy in the system and will provide a bigger time buffer for the MOI to act in the event of sabotage of the incoming water. The extra facilities should also be dispersed throughout the city. That way they will be harder to target with physical attacks.

Response

The last part of the plan will discuss what steps the MOI should take if an attack was to succeed.

In the event of a successful attack on Riyadh's water supply the Ministry should institute immediate water rationing. The amount and period of rationing will depend on the severity of the attack and the amount of time required to restore normal function of the water supply network. All reserve water should be distributed via designated distribution centers within each neighborhood and should be overseen by police presence in order to reduce unrest from the citizens. This will need to be combined with an information campaign that would inform the citizens of the situation and stressing the importance of using the water only for essential needs such as cooking and drinking.

In the case of a severe attack where water supply cannot be reestablished in short order, citizens should be evacuated from the city. This can be done by organizing car and bus

transportation for those that do not have access to them and setting up refugee camps near coastal cities who still have functioning water desalination plants. The refugee camps can be supplied with water via water trucks. The distribution of water should be overseen by police in order to reduce unrest from the citizens.

Application

This section will address the ethical and legal considerations that need to be taken into account for each portion of the proposed plan.

Prevention

Brining in external consulting companies can raise cultural challenges that can impede the effectiveness of any advisory or consulting services. Western IT firms may not be aware of Saudi specific cultural norms, such as the separation of men and women in training, or the need for female trainers to interact with female Saudi staff. Some venues in Riyadh may not even have female toilets on site. Proper site inspections and close coordination with the Western consultants are needed to ensure that the right consultants arrive properly prepared.

When creating protocols for checking work computers against security breaches, consideration must be given to acceptable levels of employee privacy. Unless there is a formal ban on any personal use of any company computer, inspecting an employee's internet browsing history or other personal files could raise ethical issues that could undermine trust between employees and management, negatively affecting adherence to IT security procedures.

Mitigation

There are numerous legal considerations around the development of additional water storage facilities. Where government-owned land in suitable areas is not available, the owners of appropriate "white land" may need to be identified and incentivized to support the development. This should be supported by the "Realty in Kind Registration Law", issued by Royal Decree No. 6 on 9/21423H; however, much land may not be fully processed under the requirements of the decree, and additional search measures may be needed, such as identifying contracts and notary publics and reviewing Ministry of Justice registers.

Response

Any response plan that involves evacuation or rationing raises ethical and legal issues. Numerous people may be reluctant to be evacuated from their homes. Forcible removals could foment civil unrest and should be avoided; equally, workers with expired iqamas or invalid visas will be reluctant to engage with authorities for fear or deportation. However, failure to evacuate populations in the event of water disruptions could lead to disease and fatalities, in turn creating a public health issue. For the benefit of limiting the consequences of an attack, water rations, medical support and evacuation and rehousing support should be made available regardless of immigration status.

Justification

This section will discuss contingencies for plan proposal.

Prevention

Training is not always 100% effective and workers can still compromise their credentials for several reasons such as growing lax, or simply not following the training. To reduce the risk of this access to crucial parts of the software systems should be restricted to higher level personal. All personal (and especially higher level personal) should have their work computers checked by IT on regular basis and should also change their log in passwords weekly.

Mitigation

A simultaneous cyber attack on multiple water treatment plants and storage facilities as well as the desalination plants would be truly devastating. If that were to happen having more water storage facilities within Riyadh would not necessarily be helpful if they all end up compromised. In order to reduce the risk of such an attack the security protocols in the different plants could be slightly altered. That way, if one place is compromised, the hackers will not be able to use the exact same method to hack the other locations.

Response

One weakness to this plan is that it may lead to unrest, maybe even looting, from the citizens if the duration of the rationing continues for too long. This can be mitigated by

keeping citizens informed and calm, as well as by increasing police presence throughout the city (or refugee centers for the evacuated citizens).

Conclusion

The overall plan is not perfect and does require the investment of money and resources, some of which will not produce a monetary return. But our duty as MOI officers is to ensure the safety and wellbeing of our citizens thus the investment in their security is well worth the money. The plan outlined in this report will increase the safety of our citizens by increasing our prevention methods against the identified threat and will also help the MOI mitigate and respond to the threat in the unlikely event that we are unable to prevent it.

References

- Argaam Special (2018, August 26). *Saudi Arabia consumed 3 bln cubic meters of drinking water in 2017*. Argaam. https://www.argaam.com/en/article/articledetail/id/567200.
- Baezner, M. (2019, May). *Iranian Cyber-activities in the Context of Regional Rivalries and International Tensions*. Center for Security Studies (CSS), ETH Zürich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20190507_MB_HS_IRN%20V1_rev.pdf.
- BBC (2019, September 17). *Saudi oil attacks: Drones and missiles launched from Iran – US*. BBC. https://www.bbc.com/news/world-middle-east-49733558.
- Jones, S., Harington, N. and Bermudez Jr., J. S. (2019, August 5). *Iran's Threat to Saudi Critical Infrastructure: The Implications of U.S.-Iranian Escalation*. Center for Startegic and International Studies. www.csis.org/analysis/irans-threat-saudi-critical-infrastructure-implications-us-iranian-escalation.
- Macrotrends (2020). Riyadh, Saudi Arabia Metro Area Population 1950-2020. Macrotrends. https://www.macrotrends.net/cities/22432/riyadh/population#:~:text=The%20current%20metro%20area%20population,a%203.57%25%20increase%20from%202017.
- Paganini, P (2020, February 9). *The number of cyber-attacks on Saudi Aramco is increasing*. Security Affairs. https://securityaffairs.co/wordpress/97527/breaking-news/saudi-aramco-under-attack.html.
- Ratcliffe, V. (2019, November 18). Attacks on Aramco Plants Expose Risks to Saudi Water Supply. Bloomberg. https://www.bloomberg.com/news/articles/2019-11-18/attacks-on-aramco-plants-highlight-risk-to-saudi-water-supply.
- Witt, R (2020). *Countries in the Middle-east Highly Vulnerable to Cyber Attacks, says PWC Study*. Naseba. https://naseba.com/content-hub/topic/cyber-security-topic/companies-middle-east-highly-vulnerable-cyber-attacks-says-pwc-study/#:~:text=There%20has%20recently%20been%20a,activity%20in%20the%20Middle%20East.&text=The%20report%20also%20found%20that,global%20average%20of%20nine%20percent.