IN ASSOCIATION WITH

MODEL ANSWER A

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.**

Assessing the Threat

There are two aspects to a standard threat assessment: likelihood and magnitude. Combined, these give a measure of risk, such that:

Risk = Likelihood x Magnitude

The first question is, what is the likelihood of an Iranian-backed cyber security attack on the water supply in Riyadh? This has several components.

A first step in intelligence analysis is the collection of Open Source Intelligence (OSINT). According to a report by PWC, businesses in the Middle East are more vulnerable to cyber-attacks then those elsewhere, with 85 percent of respondents to a survey claiming they were victims of an attack (Witt, 2020). In addition, there have been at least eight attacks on Saudi Arabian assets backed by Iran since 2012, with a peak in 2016; this is shown in Figure 1.

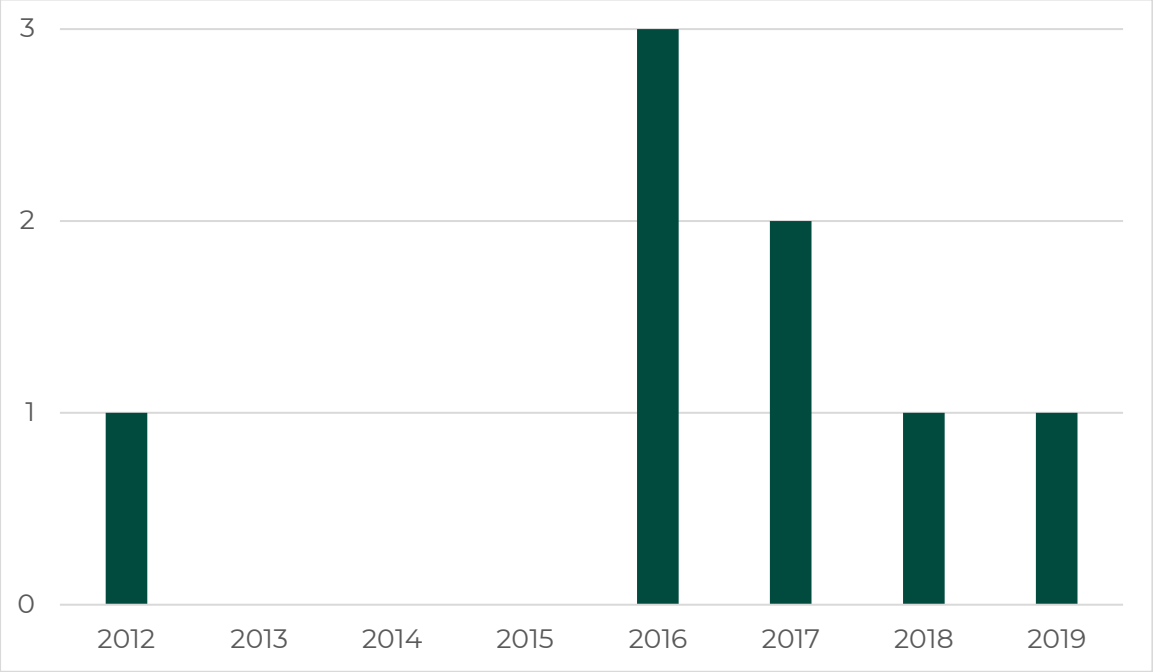

Figure 1: Count of Iranian-back Cyber-attacks on Saudi Assets (from Baezner, 2019; Paganini, 2020)

However, none of these attacks were on water-related infrastructure.

We therefore have three pieces of information to assess the likelihood of an Iranian-backed cyber-attack on the water supply:

- 85% of businesses have been subject to some form of a cyber-attack (Witt, 2020),
- Iran has backed 7 cyber-attacks on Saudi Arabia since 2016, though the trend is decreasing (Baezner, 2019; Paganini, 2020), and
- There have been no attacks on water infrastructure reported (Baezner, 2019; Paganini, 2020).

This suggests that 85% should be regarded as the absolute ceiling on the probability of an attack; the threat may nonetheless be deemed to be of high likelihood.

The second question is, what is the magnitude of such an attack?

A report from CSIS (Jones et al, 2019) claimed that

- analysts have noted that “every desalination plant built is a hostage to fortune; they are easily sabotaged”,

- Ras al-Khair, Saudi Arabia's largest desalination plant, is vulnerable to a cyber-attack, and
- an attack on the desalination plant at Jubail would force Riyadh to evacuate "within a week," as the plant provides over 90% of the city's drinking water.

The requirement to evacuate Riyadh within a week can be deemed to be highly damaging as evacuating over 7 million people will be logistically very difficult and would require large amounts of resources.

Combined, we arrive at an assessment that suggests medium-to-high likelihood and major magnitude. This is shown graphically in Figure 2.

Low Likelihood – Minor Magnitude	High Likelihood – Minor Magnitude
Low Likelihood – Major Magnitude	High Likelihood – Major Magnitude **Identified Risk Profile**

Figure 2: Risk Assessment Matrix (adapted from University of Pennsylvania)

This assessment needs to be treated with caution. There is little historical information to base an assessment of this exact threat considering the target and the attack method. Instead, comparable threats have been used and their individual likelihoods moderated against each other. This has given what can be taken as upper limits on the potential likelihood and magnitude, but with no directly comparable historical events we must base our assumptions on the available analogues.

Prevention, Mitigation and Response

Prevention

The first part of any plan is to prevent the attack from happening. This essentially reduces the likelihood from high to low.

Cyber-attacks often start with phishing: attempts to steal passwords and other access methods to the relevant computer systems. Rigorous education and training programmes should be implemented to educate all water-industry personnel on the dangers of cyber-attacks, and to train them in how to spot phishing attacks and other

attempts to compromise computer systems. These training programmes should be repeated annually to ensure new staff are taught, and old staff remember.

Cyber security consultants should also be requested to perform annual security audits of all relevant computer systems.

These training and audit programmes can easily incorporate international best practice by sourcing experts from international organizations. However, the opportunity for knowledge transfer should be seized, so that this expertise can be developed domestically within Saudi Arabia, to allow training to take place within a culturally appropriate context.

Education, training, and security audits do not provide fail safes. Staff will often compromise computer security, either accidentally by failing to properly assess the security threat of each and every email, or intentionally, by – for example – copying files from one computer to another using a USB drive. Nonetheless, these programmes can raise awareness and therefore diminish the likelihood of breaches and are thus still worth implementing. The program can also be combined with regular IT screenings of the work computers in order to ensure there have been no security breaches.

The possibility that staff will breach IT security regulations either accidentally or on purpose raises important ethical and legal questions. Legally enforceable penalties may be required to discourage staff from recklessly breaching IT security in a way that could expose the system to risk. However, if a breach does occur, it is important that the IT experts are able to respond quickly. If penalties discourage people from reporting breaches, then they may prove counterproductive. A way to solve this may be to create an anonymous reporting system. If people are caught breaching security regulations they may be punished, but breaches can be reported quickly and safely to IT experts for a rapid response.

Mitigation

The second part of the plan is to mitigate the severity of any attack. This reduces the magnitude from major to minor.

Riyadh is particularly vulnerable to attacks on water infrastructure because there is little local ground water. Desalination plants are (as discussed) easily identified and very vulnerable, outside water must be piped in over long distances.

These three aspects give three mitigation routes.

1. First, the lack of local ground water should encourage water conservation and decentralised storage measures. This requires public information campaigns to raise awareness of water conservation, stricter enforcement of water efficiency standards, and a review of water storage facilities.
2. Second, the vulnerability of desalination plants can be mitigated through increasing redundancy in the system and moving from a small number of very large plants, to a larger number of smaller plants. Unfortunately, this is a highly expensive policy, but the expense would be well justified as the plan will increase the reserve water storage capacity of Riyadh which currently stores only one day's worth of water (Ratcliffe, 2019).and provides a very limited buffer for emergencies.
3. Third, in a similar way to the second point, water pipeline networks can be strengthened with additional pipelines that can take over if there is a leak in the main pipeline. Again, this kind of infrastructure policy is highly expensive. Despite the expense, building redundancy into the system can substantially reduce the danger from any one attack.

All aspects of the plan's mitigation component will require funding and oversight from the Ministry. If funding is approved MOI officers will be required to be assigned to oversee each mitigation aspect. A legal aspect to be considered would be the land appropriation for construction of new plants or pipelines would need to go through the appropriate legal channels and in some cases might need to be purchased if it is not owned by the state.

Even if we create a larger number of smaller plants to increase water storage capacity one simultaneous cyber-attack may be used to disable them all. In order to prevent this each plant should have a separate and ideally unique firewall configuration so that an attack on one does not turn into an attack on all.

Response

The third part of the plan is to be able to respond to any attack that does occur.

Should there be a successful attack on Riyadh's water supply, the Ministry of Interior will need to coordinate with other agencies to implement an immediate water rationing system. Blue water trucks can be tasked to provide water for drinking and cooking from

centralized distribution centers set up within each neighborhood. In addition, public information campaigns should discourage the use of water for washing and cleaning. Similarly, water-intensive businesses such as laundries should be closed.

Any response plan will have serious shortcomings: the size of Riyadh's population, combined with current water usage rates means that providing an effective rationing system at short notice will be highly challenging. The alternative is to coordinate evacuations from the most affected areas, something that will raise multiple social and cultural issues. Especially difficult will be responding to ethical dilemmas raised in deciding which neighborhood must evacuate and which can remain. Depending on the severity of the water shortages both of those strategies might have to be implemented and the challenges would have to be addressed through the placement of police to reduce civil unrest during water distribution and evacuation, as well as the creation of a detailed evacuation plan that will need to be amended as needed depending on the situation.

In the case that large parts of the city needs water distributed and we lack enough water supply trucks we can requisition trucks from other cities or use alternative forms of transportation to move the water to the distribution centers.

Saudi Arabia's centralized form of government allows for quick decision making and clear leadership. This will support the implementation of these plans. However, the arid conditions, high current water use, and cultural sensitivities around social mixing during any kind of evacuation pose serious challenges the Ministry must prepare for. 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 time and money that it will cost. The plan outlined in this report will increase the safety of our citizens by increasing our prevention procedures 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

- 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.
- 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 Strategic and International Studies. www.csis.org/analysis/irans-threat-saudi-critical-infrastructure-implications-us-iranian-escalation.
- 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.