****

**CSC 5272 Assignment 1**

U.S. Magnesium – Skull Valley, Utah.

6/17/2024

Table of Contents

[Company Overview 3](#_Toc151122165)

[Module 1 8](#_Toc151122166)

[Module 2 11](#_Toc151122167)

[Appendix A: Additional Discussion Questions 13](#_Toc151122168)

[Appendix B: Acronyms 17](#_Toc151122169)

[Appendix C: Case Studies 18](#_Toc151122170)

[Appendix D: Threats 19](#_Toc151122171)

[Appendix F: Contacts and Resources 22](#_Toc151122172)

An aerial view of a factory

Description automatically generated

**U.S. Magnesium – Company Overview:**U.S. Magnesium operates the United States’ sole domestic supply of magnesium. Magnesium is a core component for the production of incendiary weaponry, metal alloying, electronics manufacture, uranium processing, food additives, and paper. According to the United States Geological Survey, the United States secures 47% of all domestic magnesium consumption from this singular facility – with all other magnesium being imported[[1]](#footnote-2). The U.S.-China Economic and Security Review Commission identified the reliance on imported magnesium from China as a key supply chain vulnerability[[2]](#footnote-3).   
  
U.S. Magnesium’s sole plant is located in Skull Valley, Utah. Due to the apt name, it advertises positions for the facility as being located in Salt Lake City, Utah despite the facility being located 60 miles away from the city center. The facility extracts magnesium from the waters of the Great Salt Lake. The facility hold a 2.7 star rating on google reviews, with many noting that toxic clouds of Mercuric Chloride would form near the ground during the winter months, magnetism sufficiently strong to deform steel-toed boots, little to no security, poor cell phone reception, noting that the facility is the #2 polluter in the state of Utah, and is a current EPA SuperFund site[[3]](#footnote-4). A 2004 Centers for Disease Controls survey of employees found that most workers reported respiratory irritation from exposure to chlorine gas, and that all workers surveyed had an increased amount of hexachlorobenzene in their blood compared to the general population[[4]](#footnote-5).   
  
U.S. Magnesium also operates a sales office which also is involved with personell management (Human Resources). This office is located in Salt Lake City, Utah – 60 miles away from Skull Valley.

The magnesium separation process involves high temperature electrolytic cells of molten salt and chlorine gas used to separate out the magnesium. The residue from this process is the sodium from the molten salt, which is an explosive risk when exposed to water. Magnesium is also noted for its explosive properties[[5]](#footnote-6). What could the risk be of a computerized control system operated by disgruntled poisoned employees that manages chlorine gas, magnesium, and sodium at high temperatures for the production of a material critical to the U.S. supply chain? What could possibly go wrong?

# Module 1

### Day 1

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Federal Aviation Administration (FAA) release a joint report addressing increased unmanned aircraft system (UAS) activity near chemical sector facilities across the U.S. The report provides details on specific incidents, including a chemical plant that found a grounded drone with a memory card containing footage of the facility, and a drone operator caught taking photos of a pipeline.

In addition to hostile surveillance, smuggling, disruption, and weaponization, the report stresses adversaries may illegally use UAS as a mobile platform to interrupt or modify digital services or gain unauthorized access to data systems. The report encourages increased vigilance for UAS activity and directs chemical sector infrastructure owners and operators to report suspicious activity to their local FBI Field Office.

## Discussion Questions

1. What are the greatest cybersecurity threats to your organization?  
     
   Physical Attack – Though the workforce is adequately compensated, workplace dissatisfaction means that insiders with access to computer systems are a strong possibility. The nature of large scale industrial production also means that subcontractors will have access to facility hardware. Furthermore the lax security procedures present mean that unknown visitors come and go through the facility

Social Engineering Attacks – The largely labor intensive portion of our workforce means that most workers at U.S. Magnesium are unlikely to be technologically inclined, and may therefore be vulnerable to phishing or baiting that sound authoritative. Furthermore the aging nature of the facility and frequent layoffs mean there is a lack of institutional knowledge preserved to ensure knowledge of internal procedures.

Supply Chain Attacks – The relatively small size of U.S. Magnesium means that it is dependent on vendors for providing services such as payment services, maintenance, machinery operations, personell management, and general I.T. services.

Man-In-The-Middle-Attacks. The spread out nature of the Skull Valley facility means that communications had previously been managed through direct wired connections. However, to save money due to the corrosive properties of the ever present chlorine gas clouds communications and management of all equipment is being handled through unencrypted wireless network between buildings and equipment.  
  
Denial-of-Service Attacks – The aging hardware of the Skull Valley facility has no protections against DDoS attacks. Hardware was procured for a physically wired system where external attack was not envisioned and has been hastily retrofitted to the new wireless system to save money on installation and frequent repairs.

1. What cybersecurity threat information does your organization receive?
   1. What threat information is most useful?  
        
      The most useful information would be indication of the presence of vulnerabilities within the existing information technology infrastructure employed by U.S. Magnesium. It would also be useful to be provided a list of vendors that are known to be compromised.
   2. How is information disseminated to the relevant parties within your organization?  
      Information is gathered by the head of IT department who has recently been replaced following the recent layoffs and is thus unaware of the security landscape of the Skull Valley facility. The head of security plans to “call the plant manager if anything goes wrong”, and believes it would be the plant manager’s decision whether or not to inform anyone else. While there should be a communications plan regarding cybersecurity threats, the ‘old-school’ nature of the facility means that lines of communications regarding cybersecurity threats have not been established and information regarding them is mostly spread through word-of-mouth.
   3. What actions would your organization take in response to the report like the one presented in the scenario?  
      The head of IT would likely make a mental note, and inform no one, finding it mildly interesting. It is unlikely that the head of IT would actively be looking for such reports unless they appeared in their news feed.
2. Discuss your organization’s cyber resilience planning.[[6]](#footnote-7)
3. What risk assessments have you conducted to identify specific cyber threats, vulnerabilities, and critical assets?[[7]](#footnote-8)

A competent organization would have performed a vulnerability assessment to identify and prioritize vulnerabilities in the IT system, and networks. A competent organization would also have performed a threat assessment to identify the potential threats that could exploit said vulnerabilities. A competent organization would have also performed risk assessment to determine the most critical assets based on potential damage to those assets. However, U.S. Magnesium is not such an organization, but knows that a cybersecurity breach would be ‘bad’ and could ‘cause a lot of problems’.

1. Describe your asset management plan and how you prioritize critical assets.  
   A good asset management plan would create a list of all hardware, software, data, and network assets; assess the value of each asset; determine responsibility for each asset within the company; and prioritize the upkeep of a particular asset depending on the value of each asset dependent on that asset.  
     
   However, assets have been prioritized by the accounting team. The excel spreadsheet wizards at accounting have concluded that the sales team is the most valuable asset within U.S. Magnesium as they ‘produce all the income’.
2. What improvements have you implemented to enhance cyber resilience following recent risk assessments?  
   U.S. magnesium should have implemented a continuous monitoring system for spotting unmanned aerial vehicles around the facility and provided hardening of the unsecured wireless communications systems in the facility and implemented authentication.   
     
   Instead, the head of I.T. assures us he is ‘on it’.  
   1. Does your organization apply Zero Trust Architecture (ZTA)/zero-trust concepts?[[8]](#footnote-9)  
      No.U.S. Magnesium does not employ any Zero Trust concepts. It is the firm belief of U.S. Magnesium that if someone has a password then they are the person who ought to have the password. Access is permanently granted after review by I.T., limited risk assessments are made, and I.T. services not provided by third-party-vendors are all self managed. Multi-factor authentication is not employed. If it has worked until now, why wouldn’t it keep working?

### Day 2

Your IT department authorizes the installation of an “automated software update” on one of your critical systems.

1. Describe your organization’s network configuration and your approach to network segmentation of IT and OT systems.
   * + - 1. Describe your organization’s patch management and vulnerability management plans.  
              
            While a good patch management plan would try to ensure that all devices and software are up to date with the latest security patches, and push security patches after identifying the impact of the new patch, the I.T. department at U.S. Magnesium provides updates when the notification of the application prompts them to.  
              
            There is no vulnerability management plan at U.S. Magnesium. There are no automated scanning of the network, systems, and application for vulnerabilities, and as a result there is no prioritization of vulnerabilities or mitigation strategies.

### Day 3 – 5:00 a.m.

Your organization’s security team receives a report from an employee who observed a drone appear to drop something near your facility’s central building before losing sight of it. Soon after, the IT department notices a new Media Access Control (MAC) address associated with a known UAS manufacturer attached to their network and narrows its location to inside the perimeter.

1. What UAS detection capabilities and techniques does your organization employ at your facility?
   1. How would your organization respond if an unrecognized UAS lands within your facility perimeter?  
        
      Security guards would likely assume any UAW was meant to be there for providing aerial surveying of the facility and would not report it to anyone.
   2. How would physical security and IT security coordinate response?   
        
      Security is unlikely to communicate with IT security directly. U.S. Magnesium considers physical security and IT security separately, so coordination would be handled by the plant manager. Unfortunately this means that if physical security is unable to identify a IT security threat, they would likely not report it to the plant manager. Similarly, due to the plant manager’s unfamiliarity with IT, they would be unlikely to pass on the information to IT Security. Spotty cell-phone reception in Skull Valley means that reporting anything would require security to physically move to talk to IT security, and due to the temperature and chlorine gas clouds, physical security is unlikely to get up to make a physical report.

### Day 3 – 6:00 a.m.

Upon arriving at one of your facilities, an employee picks up a USB drive with the company logo on a walkway within the facility perimeter.[[9]](#footnote-10) The employee connects the device to their company computer and opens a file with embedded links.[[10]](#footnote-11) They click one of the links and receive a “404 – Not Found” error message. After receiving the error message, they unplug the drive and throw it away.[[11]](#footnote-12)

1. What policies and procedures does your organization have to maintain the security of facilities, networks, and systems?
   1. What policies do you have regarding company-issued devices and removable media?  
      The previous IT manager at U.S. Magnesium established a policy regarding not plugging in any removable media to computers at work.
   2. Where are these policies and procedures documented?  
      This policy is documented within the onboarding training that IT provides to all workers when setting up their accounts. This policy however is not written in any contract or employee handbook.
   3. How is physical access managed?  
      Doors in the facility are locked using physical keys. However due to corrosion from chlorine gas many of the doors appear to be locked even when the lock has not been turned. This means many doors at the U.S. Magnesium facility in Skull Valley are not actually locked.
   4. How is IT and OT access managed?  
      Users are onboarded using the Windows Group Policy Management Console which allows users to be restricted in access to files and systems based upon their user roles. User accounts are reviewed when IT remembers. It is not unusual for an employee who has departed U.S. Magnesium to still have a valid account to access IT services. Operational Technology to hardware in facility is access granted through a single password that is the same for all devices. The idea is that this password is known only to the technicians operating the hardware.
2. Describe your organization’s cybersecurity training program for employees.[[12]](#footnote-13)
   1. How often are employees required to complete this training?  
      Employees are required to undergo cybersecurity training during onboarding, and only during onboarding. This means employees are not kept aware of cybersecurity threats. The partioning of the sales office and personell management at the sales office in Salt Lake City means the IT team (which is primarily concerned with hardware in the Skull Valley Facility) is not intimately involved with the Salt Lake City Office.
   2. Describe the cross-training or the coordination between the IT and OT departments.  
      The departments are one and the same. Cross-training is performed by shadowing existing members of the IT department. This proves problematic during layoffs as the lack of documentation means institutional knowledge is frequently lost.
   3. What additional training is required for users with system administrator-level privileges?  
      None. Administrator level users are assumed to know what they are doing even if this is not the case.
   4. Does this training address removable media?  
      The onboarding training does address removable media – it states to not plug in any removeable media to any company computer.
3. Has your organization conducted a risk assessment to identify specific cyber threats, vulnerabilities, and critical assets?
   1. What IT and OT systems or processes are the most critical to your organization?   
      The most critical part would be the OT process that allows the technicians in the control room to control facility machinery remotely. The next most critical part would be the payment processing system provided by third-party vendors.
   2. Describe your organization’s asset management plan and how you prioritize critical assets.  
      The organization’s asset management plan is primarily controlled by the accounting team. The accounting team has decided that assets are valued based upon the amount of income that they bring into the company. This value is then used as the basis for prioritization with up-time being the primary judge for how well such an asset is performing. This asset management plan does not determine critical assets based upon the reliance of other assets upon that asset, nor the potential damage that could occur if something were to happen to that asset.
   3. Does your organization have a vulnerability management program dedicated to mitigating known exploited vulnerabilities in internet-facing systems?   
      No.
   4. How are insider threats integrated into your risk management efforts?  
      A system that monitors employee network actions and flags unusual activity would be ideal for determining when an insider may be a threat. However, management seems to believe that frequent layoffs mitigate the risk of insider threats as employees are laid off before they fully understand the systems they have access to.
4. What tools (e.g., threat hunting, security audits) do you leverage as part of a proactive cybersecurity strategy? [[13]](#footnote-14)   
   The cybersecurity strategy at U.S. Magnesium is purely reactive. The combination of the IT team with OT means that staff are overworked and spend most of the time providing upkeep to hardware. All expenses to subscribe to services that would provide protection against cybersecurity threats would otherwise have to be run through accounting who will not approve “non-essential maintenance services”.

### Day 6

Technicians responsible for monitoring the sensors on the chemical storage tanks notice anomalous readings. Upon inspection of the storage tanks and sensors, no specific cause of the anomalous readings is identified. The technicians replace the sensors and the readouts on the ICS/SCADA monitors return to normal.

1. How does your organization baseline network activity?[[14]](#footnote-15)
   1. How do you distinguish between normal and abnormal traffic?  
      Abnormal traffic is distringuished from normal traffic based upon a baseline comparison. I.e. if only a certain number of types of request are sent each day, then any traffic different from that amount is abnormal.
   2. What are your next steps when abnormal activity is detected/reported?  
      When abnormal traffic is detected, the next step is to shut down the source of that abnormal traffic. This might been suspending a service, locking out a user, or blacklisting a wireless router.
   3. What Indicator of Compromise (IOC) feeds does your organization use?  
      U.S. Magnesium does not use any subscription based services. However, some members of IT do pay attention to the Industrial Control Systems alert from the Cybersecurity on Infrastructure Security Agency. CISA also provides convenient cybersecurity goal assessments and vulnerabity assessments.
2. How do employees report and log anomalous IT/OT activity?
   1. How does your IT/OT department respond to reports of widespread problems?  
        
      Anomalous traffic typically results in an automatic shutdown of the source of the problem. In the event of the error being a service an older version of the service may be put into place, or the service deleted entirely from the system and reinstalled. For anonmalous user activity all account permissions are suspended until the source of the problems can be determined.
3. How do IT/OT and physical security teams coordinate their investigation into potential incidents impacting both physical and cyber security?   
   IT/OT does not coordinate with physical security. Security handles physical locks and unknown employees based upon their identification badge. IT/OT handles electronic systems. IT/OT managers however have found it helpful to get to know security guards personally so requests can be made of them. Coordination of the two is handled through the plant manager.

# Module 2

### Day 22

Staff discover a misconfigured firewall allows access to both IT and OT systems. Staff trace the issue to an incorrectly installed update.

### Day 23

An individual arrives at your facility and states they are a new employee from your ICS/SCADA device service vendor. The individual is allowed access to the facility. They connect their device to the facility’s network and multiple ICS/SCADA devices before leaving.

## Discussion Questions

1. What level of access do your third-party vendors have to your organization’s network?[[15]](#footnote-16)
   1. How often are third-party access rights and data logs reviewed?  
      Though Third Party Access rights and data logs should be reviewed daily while the Third Party has access to any U.S. Magnesium Facilities, access rights are actually reviewed whenever those in IT remember to do so. A schedule would very much help them ensure proper security.
   2. What mechanisms or processes are in place to prevent malicious activity?   
      IT is fortunate enough to be in charge of what is installed on U.S. Magnesium’s systems. Therefore no third-party software is installed without first performing a risk assessment, and imposing security controls that manage access privileges for any third-party vendors. Privileges are typically granted for only a limited time period with the idea that third-party vendors have to pester IT to receive renewed access rights.

### Day 24 – Morning

An alarm is triggered, notifying employees in the control room that sensors are malfunctioning. Staff hurry to the liquid chemical storage tanks and take manual readings. The readings reveal numerous abnormalities. While trying to make the adjustments at the control panels, staff realize every panel in the control room is unresponsive.

### Day 24 – Mid-morning

Additional staff are called to report to work as the facility attempts to go to manual operations. Upon arrival, staff cannot use their key cards to enter the facility, and closed-circuit television (CCTV) cameras are not working.

1. What are your procedures for addressing unresponsive ICS/SCADA control panels and nonoperational sensors?
   1. Where are these processes documented?  
      Though processes should be documented in a convenient manual that comes with training employees, no such manual currently exists at U.S. Magnesium. It Is assumed that the workers will go to take readings from physical sensors.
2. What redundant systems exist for when primary systems are compromised?
3. What alternative systems or manual processes do you implement to continue operations if a critical system is unavailable for a significant period?   
   Manual controls exist for all facility operations. These manual controls are not hooked up to any electronic systems. Should the systems need to be shut down, a lockout-tagout system is in place to ensure that machinery stays off when it’s meant to stay off.
4. Who can authorize use of alternate systems or procedures?  
   Manual controls are not obstructed. The plant manager or shift supervisor for any system can authorize use of manual operations.
5. How long can you perform manual or alternate processes on your critical systems?  
   The manual control nature of the system means manual operations can continue indefinitely – however it will slow down production significantly.
6. What resources do you have for additional staffing requirements?   
   In the event that more staff are required, existing staff can be required to perform overtime. It should be noted that U.S. Magnesium already has significant mandatory overtime for its existing employees due to current staffing issues.

### Day 24 – Afternoon

While conducting visual examinations of the chemical storage tanks, an employee notices one tank has a considerably lower volume than it had an hour ago. A system alarm alerts facility operators of several control valves opening and closing at random times. Attempts to close the valves via the ICS/SCADA controls do not work.

1. Using your organization’s cyber incident response plan (CIRP), describe the actions your organization would take to minimize impact on current operations.
   1. How does your plan define escalation criteria, notifications, activations, and/or courses of action?

Escalation criteria is determined based upon the value of the asset impacted, and the severity of the impact to the asset. Whenever there is an incident, all staff that use the impacted asset are notified of the impact via email, if the asset is high value enough then the plant manager is notified.

* 1. What guidance does the plan include on assessing the severity of the incident?  
     The severity of the incident is based upon the potential impact of the incident. This potential impact is usually assessed by the the asset impacted – to be clear this means severity is based purely on the asset impacted – not upon the actual impact to the asset itself.
  2. How does incident severity level dictate response?[[16]](#footnote-17)   
     The higher the severity level the more immediate the response. Extremely severe incidents result in immediate safety shutdowns of impacted assets.
  3. How are critical systems and processes incorporated within your plan?  
     Critical systems and processes are given the highest level of attention. Even if an incident does not apparently impact a critical system and process, the first response is to check critical systems and processes to determine if there is any residual impact. It is possible that vulnerability assessments did not account for everything, and critical processes could be at risk.

1. How does your CIRP/IT response plan incorporate OT incident response?
   1. Is your CIRP aligned with any OT incident response plans?  
      Yes, CIRP responses to hardware trigger OT incident response plans such as switching to manual operations if electronic controls are in danger.
2. What information are you sharing internally (e.g., employees, leadership)?   
   Information shared internally includes what asset was impacted, the severity of the impact, and an estimated time until the impacted asset is back in regular operation based on past experience.
3. What information are you sharing externally (e.g., customers, vendors)?
   1. What sector partners do you collaborate with before, during, and after a cybersecurity incident?  
      U.S. Magnesium has signel up to connect with its CISA Regional Cybersecurity Advisor to try to gets heads up on incidents occurring in the area and similar threats that could occur to U.S. Magnesium. Incident reports are also filed with CISA during and after security incidents.
   2. What actions can your organization take to mitigate reputational impacts because of these incidents?  
      The best way to mitigate reputational impact is to have continued operations. It is important for customers to see that U.S. Magnesium is capable of delivering product safetly even during system outages.
4. What legal and regulatory notifications are required based on the scenario?
   1. When would notifications be made and who is responsible for making the notifications?  
      The head of IT is responsible for making all notifications. Notifications are not required to be made to DHS or CISA, however they should be.
5. Based on the discussion, what changes will you implement to increase the resilience of your organization against future attacks?

# An organization’s protection against future attacks is only as good as the capability of the organization to understand future attacks. U.S. Magnesium has a poor understanding of cybersecurity due to it being a legacy manufacturing company. Convincing the company that change is required is the hardest part. As an outsider the best way to convince management that change is necessary may be contact ing a government agency such as CISA, OSHA, or the EPA who wield power over management and convincing them of the legal risk damages from a cybersecurity incident may impose. Once convinced of this importance, it may then be possible to subscribe to vendors that offer more robust vulnerability analysis, and create mandatory yearly training in cybersecurity risks. This would also enable installing direct lines of communication, and hiring more staff to set up systems for encryption of local networks to protect against attacks. This may also allow asset management plans to be formulated based upon actual risk as assessed by technical personell instead of by accountants who are unaware of the actual inner workings of the facility.

1. Mineral Commodity Summaries 2023, 2023, pubs.usgs.gov/periodicals/mcs2023/mcs2023.pdf. [↑](#footnote-ref-2)
2. Section 4: U.S. Supply Chain Vulnerabilities and Resilience, www.uscc.gov/sites/default/files/2022-11/Chapter\_2\_Section\_4--U.S.\_Supply\_Chain\_Vulnerabilities\_and\_Resilience.pdf. Accessed 17 June 2024. [↑](#footnote-ref-3)
3. “US Magnesium Site Profile.” EPA, Environmental Protection Agency, 20 Oct. 2017, cumulis.epa.gov/supercpad/SiteProfiles/index.cfm?fuseaction=second.cleanup&id=0802704#:~:text=Facility%20operations%20and%20waste%20disposal,threat%20to%20birds%20and%20wildlife. [↑](#footnote-ref-4)
4. HHE Report No. Heta-2004-0169-2982, U.S. Magnesium, ..., www.cdc.gov/niosh/hhe/reports/pdfs/2004-0169-2982.pdf. Accessed 17 June 2024. [↑](#footnote-ref-5)
5. Telgerafchi, Armaghan Ehsani, et al. “Magnesium Production by Molten Salt Electrolysis with Liquid Tin Cathode and Multiple Effect Distillation.” Frontiers in Chemistry, U.S. National Library of Medicine, 3 July 2023, www.ncbi.nlm.nih.gov/pmc/articles/PMC10351870/. [↑](#footnote-ref-6)
6. CISA CPG Checklist, “2.S Incident Response (IR) Plans,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-7)
7. NIST CSF Tools, “Identify Critical Assets,” <https://csf.tools/reference/nist-sp-800-53/r5/cp/cp-2/cp-2-8/> [↑](#footnote-ref-8)
8. CISA Resources, “Zero Trust Maturity Model,” <https://www.cisa.gov/zero-trust-maturity-model> [↑](#footnote-ref-9)
9. CISA – News & Events, “Using Caution with USB Drives,” <https://www.cisa.gov/news-events/news/using-caution-usb-drives> [↑](#footnote-ref-10)
10. CISA CPG Checklist, “2.V – Prohibit Connection of Unauthorized Devices,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-11)
11. NIST CSF Tools, “MP: Media Protection,” <https://csf.tools/reference/nist-sp-800-53/r5/mp/> [↑](#footnote-ref-12)
12. CISA CPG Checklist, “2.I – Basic Cybersecurity Training,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-13)
13. CISA, “Cyber Resource Hub,” <https://www.cisa.gov/cyber-resource-hub> [↑](#footnote-ref-14)
14. CISA CPG Checklist, “2.O Document Device Configurations,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-15)
15. NIST CSF Tools, “AC: Access Control,” <https://csf.tools/reference/nist-sp-800-53/r5/ac/> [↑](#footnote-ref-16)
16. CISA CPG Checklist, ”2.S Incident Response (IR) Plans,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-17)