



Martin Yarborough and Associates
8451 Deerwood Forest Dr
Fort Worth, TX 76126

Phone: (817)952-9993
Fax: (817)887-3371

FACILITY RISK ASSESSMENT – PIERCE LIBRARY DATA CENTER

2018

Risks, Threats, and Vulnerabilities | Martin Yarborough

Table of Contents

.....	1
Table of Contents.....	2
Executive Overview.....	3
Scope	3
Approach.....	3
Interviews.....	3
Summary of Findings.....	4
Facility Responses and Findings.....	4
Facility Risk Assessment Data	4
Pierce Library Data Center	4
Previous Disruptions (Historical Events)	4
Preventative Measures to Minimize Disruptions	5
Risks and Vulnerabilities	7
Natural Risks.....	8
Man-Made Risks	9
Environmental Risks.....	10
Facility Risk.....	11
Conclusion	11

Executive Overview

The primary goal of the Risk Assessment (RA) was to help Eastern Oregon University identify, analyze, and weigh all the potential risks, threats and hazards that currently exist in the business’s internal and external environments.

The RA identified if a facility is vulnerable to weather related events, HVAC failure, Internal/External Security vulnerabilities and local area hazards. By identifying the threats, Eastern Oregon University can concentrate on developing and implementing strategies for mitigation or reducing the level of threats. Eastern Oregon University can also implement strategies for contingency planning based on the potential exposures and the losses associated with them.

The objectives of the RA were:

- Identify and rank potential risks and threats
- Identify how vulnerable Eastern Oregon University is to risks and threats
- Estimate potential impact of risk
- Define preventative measures that are currently in place
- Determine the overall risk to Eastern Oregon University

Scope

The scope for the Eastern Oregon University RA included the following owned, leased, rented, occupied, etc., facilities; where business operations are conducted:

- Data Center, Pierce Library, One University Blvd, LaGrande OR 97850

The main focus was on the potential Natural, Man-Made (human) and Environmental (technology/facility) based risks that currently exist in each facility or the surround facility environment. Weather patterns, surrounding environments, previous incidents and disruptions, current policies, procedures, etc.; were all used in conducting this risk assessment.

Approach

To start the RA process, an electronic questionnaire was distributed to each manager or director responsible for facility operations. The facility representative completed the RA to the best of their ability (while obtaining help from other knowledgeable people). The purpose of the questionnaire was to identify the potential risks, threats and vulnerabilities.

Interviews

Martin Yarborough and Associates conducted collected questionnaires with the following facilities and representatives.

Facility Address	Facility Representatives	Title / Position
Pierce Library , EOU	John Garlitz	Director of Facilities

Summary of Findings

This report is intended to present management with an account of the potential risks and vulnerabilities to all Eastern Oregon University owned, leased, rented and/or occupied facilities. Additionally, this report provides a collective synopsis of risks across all of Eastern Oregon University facilities. This information can be applied toward justification and implementation of preventative measures, mitigation activities, and recovery strategies for contingency planning.

Facility Responses and Findings

Detailed information gathered by the consulting firm with the support of the facility manager(s) has been provided in the following sections. Since several data gathering methods were used, a high-level overview of each facility has been documented. Many of the findings in this report are recorded exactly as they were captured from surveys and interviews. However, some statements made by Eastern Oregon University employees have been re-worded for clarity.

Facility Risk Assessment Data

Pierce Library Data Center

- The Pierce Library Data Center is responsible for providing a primary data center and replication site for Eastern Oregon University. It is important to note that the facility provides no support for healthcare and is primarily a facility for an education setting.
- The review was conducted by Martin Yarborough and Associates in the Spring of 2018. Participating in the process was John Garlitz, who is responsible for the overall management of the Maintenance and Facilities department at Eastern Oregon University. The following risks and threats were identified during the risk assessment process.

Previous Disruptions (Historical Events)

The facility has in the past experienced disruptions, prolonged outages, and loss of services due to the following incidents.

- Water leaks

Summary of Previous Disruptions

The facility manager reported that the following disruptions have previously occurred and provided information based on those outages.

Water Leaks – the facility last experienced a water leakage in 2017 and another in 2014. The event was significant and rendered the facility non-operational for 14 days to restore functionality of the facility

Preventative Measures to Minimize Disruptions

Where appropriate, recommendations to mitigate disruptions are provided in red.

Hazardous Materials

- Hazardous materials are not stored in the Pierce Library Data Center.
- Following State Fire Marshall Reporting procedures, the policy for managing hazardous materials is reviewed annually even though currently no hazardous materials are stored.
- Spill kits are available should hazardous materials be stored in the facility.
- A yearly inventory of hazardous materials is provided to emergency services. Should hazardous materials be stored in the facility, this would be noted on the annual inventory.

Fire Containment

- The local fire department is available within 5 miles
- Annual inspections confirm that working heat and smoke detectors are in place.
- Fire dampers are used in the facility.
- The facility is constructed of concrete materials rated for fire prevention.
- Fire rating doors are used in the facility.
- An emergency preparedness plan has been developed by the Campus Security Department and approved by the governing board to manage evacuations in the event of fire.
- Designated building management staff are aware of the physical location of fire sprinkler cut-off valves.
- As per code, 2 fire extinguishers are located within the facility and the location is known by building personnel.
The fire extinguishers are identified clearly with visible signs.
- The fire extinguishers meet ABC classification and are acceptable for use in the data center in the event of a fire.
- Building personnel are trained in the use of fire extinguishers annually.
- As per fire code, annual inspections of the fire extinguishers are made on a known schedule.

Emergency Notification, Evacuation, Alarms and Exits

- Emergency alarms are located in the work area. Procedures for managing the alarms are documented. There is an annual inspection of the alarms and review of the procedures.
- Staff are provided annual training on response procedures for different types of alarms.
- All alarms are monitored both internally by facility staff and externally by first responders (police and fire).
- Alarms are powered on separate dedicated electrical circuits with UPS protection provided on the monitoring tools.
- There are “muster” locations defined in the emergency preparedness plans for personnel to gather in the event of an alarm.
- Emergency lighting is provided in the facility in the event of loss of electrical services facilitating an escape from the premise.
- A documented communication plan is provided to notify employees of any incident that may require actions.

Facility, Features, Security and Access

- The facility does NOT undergo annual structure assessments. **Recommendations: Annually inspect the facility with a contracted engineering firm to ensure structural integrity.**

- All exterior doors are securely locked with a keylock mechanism to prevent unauthorized access. **Recommendation: Proximity card access would provide documentation of ingress and egress from the facility. Backed with video surveillance, IT and campus security would be able to identify any unauthorized activity in the data center.**
- Doors to the data center are not alarmed to identify a potential “break-in”. **Recommendation: Install motion-detection that must be dis-armed after a 15 second delay to lower chances of a break-in.**
- There are no mechanisms in place to log or identify any and all entry into the data center. **Recommendation: Proximity card access, visitor sign-in sheets, an escort and tailgating policy should be implemented and monitored for compliance.**
- External video surveillance and adequate lighting for enhanced video identification are in place and monitored.
- The data center does not have moisture/water detection tools in place and have had extensive water leaks in the past. **Recommendation: Install and monitor water detection products in a central monitoring facility.**
- By directive and practice, the data centers are not used to store products, janitorial supplies or unused equipment which could restrict the ability for a clean evacuation.

Heating, Ventilation and Cooling (HVAC)

- HVAC alarms are in place and reviewed on a daily basis.
- In addition to HVAC alarms, a temperature alarm is part of the review. The alarms are monitored on a 7X24 basis with alerting in place.
- The alarm package does not include humidity sensors. **Recommendation: Install humidity sensors into the facility and maintain a constant humidity to reduce static discharge and potential electrical failure.**
- All overhead HVAC is equipped with drain pans and proper drainage to prevent the accumulation of condensation.

Utilities

- The data center has backup electrical power through a UPS and electrical generator.
- All generators are tested on a monthly basis under full load.
- Steam services are available and used for heating.

Data Center

- Backup power strategies for the data center are defined, documented and reviewed monthly.
- Generator power is tested monthly.
- All data backups are kept on-site. **Recommendation: Replication of data occurs from the Pierce data center to the Pierce Library data center. This will facilitate a quicker restoration in the event of loss of data but could be an issue should data be corrupt, lost or damaged due to unforeseen issues. Replication of data should occur over the cloud to a facility at least 150 miles from the primary/secondary data storage. Another option is to offload the SAN devices to a tape drive and move archival tapes off-site to a secure location protected from outside intervention, weather, tampering or accidental destruction.**
- Contracts, MOU or SLAs are in place with utility companies and vendors to assist in responding to an emergency.
- Fire suppression is in place (Halon) in the data center. **Recommendation: When possible, convert the Halon environment to an alternate chemical such as FM200, compressed air or other products. Halon is very corrosive and presents a significant hazard to human life.**

Risks and Vulnerabilities

Each risk or threat identified by the facility manager(s) was assigned a value for the following categories:

- Probability of Occurrence
- Vulnerability to Risk
- Potential Impact to Company
- Preventative Measures in Place

The following equation was used in determining the overall risk rating for each potential threat.

$$\text{Risk} = \text{Potential} * \text{Severity}$$

The following table explains the Rating and associate level of Risk:

Ranking	Risk Level
0	No Risk
1 – 3	Low Risk
4 – 6	Medium Risk
7 – 9	High Risk
10+	Extreme Risk

Natural Risks

Natural risks are typically associated with weather related events: flooding, high winds, severe storms, tornado, hurricane, fire, d snow storms, and ice storms. In each RA Survey, the facility(s) manager was asked to identify potential natural risks and rate the severity of each. The overall risk for natural issues is 1.9 constituting low risk.

Summary of Natural Risks

For the location of this facility and historical weather patterns, it has been stated that fire, ice and flood pose the biggest threat.

How the risk ranking was determined: **Overall Risk = Probability * Severity (|Magnitude – Mitigation|)**

Threat / Risk	Probability	Magnitude	Mitigation	Overall Risk
Drought	2	0	1	2
Earthquake	1	5	2	3
Fire	2	4	2	4
Flood / Flash Flooding	2	4	2	4
Hurricane / Tropical Storm	0	3	1	0
Ice Storms	3	3	2	3
Landslides	1	3	2	1
Severe Thunderstorms	2	3	2	2
Tornado	0	3	1	0
Wildfire	2	3	2	2
Wind (High / Severe)	2	3	2	2
Winter Storms (Severe)	3	3	3	0

Man-Made Risks

Man-made risks are typically associated with man-made type of events: bomb threats, vandalism, terrorism, civil disorder, sabotage, hazardous waste, work stoppage (internal/external), and computer crime. In each RA Survey, the facility(s) manager was asked to identify potential man-made risks and rate the severity of each. The overall risk for man-made issues is 3.66 which is a medium risk.

Summary of Man-Made Risks

For the location of this facility and surrounding area, it has been determined that civil disturbance, power failure and spills pose the biggest threat. It should be noticed that even though bomb threats, dam failures and terrorism are low, they are also very hard to predict. However, these risks should still be kept in scope for planning and mitigation strategies.

How the risk ranking was determined: **Overall Risk = Probability * Severity (Magnitude – Mitigation)**

Threat / Risk	Probability	Magnitude	Mitigation	Overall Risk
Bomb	0	6	1	0
Civil Disturbance	1	3	1	2
Dam Failure	0	5	1	0
Electrical Failure (Building)	2	3	3	0
Hazardous Spill	1	2	3	1
High Crime Area	1	2	2	0
Power Station Failure	1	3	2	1
Terrorism	0	6	2	0
Work Stoppage / Strike	1	2	2	0

Environmental Risks

Environmental risks are typically associated with exposures to surrounding facilities, businesses, government agencies, etc. In each RA Survey, the facility(s) manager was asked to identify potential natural risks and rate the severity of each. The overall risk for environmental issues is .7 and is very low.

Summary of Environmental Risks

For the location of this facility and surrounding area, it has been determined that the governmental agencies and dams/reservoirs and airports pose the biggest threats due to previous historical events.

How the risk ranking was determined: **Overall Risk = Probability * Severity (Magnitude – Mitigation)**

Threat / Risk	Probability	Magnitude	Mitigation	Overall Risk
Nuclear Plant	0	3	1	0
Hazardous Materials Plant	0	3	1	0
Hazardous Cargo Hwy	1	2	2	0
Refineries	0	3	1	0
Rail Lines	1	2	1	1
Military Bases /	0	1	1	0
Military Storage	0	1	1	0
Airports	1	2	1	1
Dams, Reservoirs, Rivers	1	3	2	1
Government Agencies	2	2	0	4

Facility Risk

Facility risks are typically associated with risks within the facility, data center, HVAC failure, technology outages, telecommunications failure, and power failure. In each RA Survey, the facility(s) manager was asked to identify potential natural risks and rate the severity of each. The overall risk for facilities is 2.11 and is low.

Summary of Environmental Risks

For this facility, it has been determined that telecom failure, and water leaks pose the biggest threats due to previous historical events and lack of preventative measures in place.

How the risk ranking was determined: **Overall Risk = Probability * Severity (Magnitude – Mitigation)**

Threat / Risk	Probability	Magnitude	Mitigation	Overall Risk
Hazardous Materials Stored Onsite	1	4	3	1
Power Failures	2	3	3	0
Telecommunications Failures	2	4	1	6
Fire System Failures	2	2	3	2
HVAC Failures	2	2	3	2
Water Leaks	2	4	2	4
Security Surveillance Failures	2	2	3	2
Adequate Lighting Failures	1	2	3	1
Alarm System Failures	1	2	3	1

Conclusion

The consultant discovered that the data center at Pierce Library are at minimal risk. The average risk is 2.1 which is low. Even though low risk is observed, recommendations to improve the risk are provided in red above and should be considered to further low risk and approach the 0 risk level.