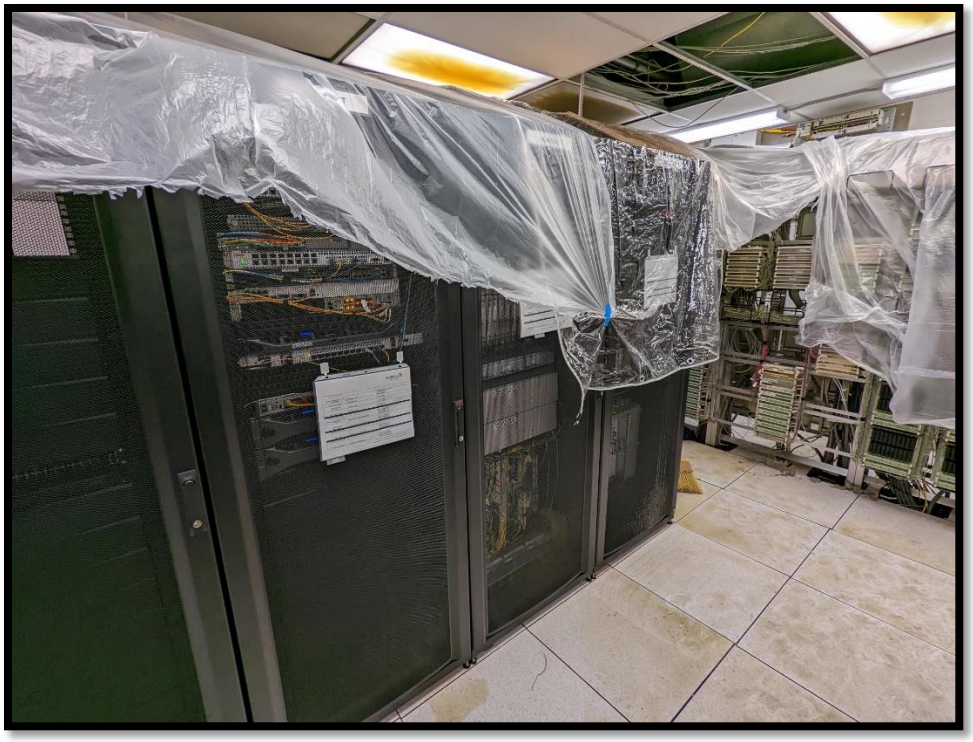

Internet Connectivity Outage Event
November 10, 2022
After Action Report

Executive Summary

On the morning of November 10, 2022, a pipe failure over the data center in the Blair-Shannon residence hall caused the loss of internet connectivity for Missouri State University and other public agencies within southwest Missouri. The failure was immediately found by network and telecommunications staff and mitigation efforts began. Maintenance and residence life staff arrived within ten minutes and senior leadership of facilities management and information services were on scene within 15 minutes of the failure and five minutes later, the notification of senior university leadership began.

The first Missouri State Alert to the campus was issued one hour after the pipe failure. Texting was the primary mode of communication both individually, and eventually text groups were created and used to communicate to the Policy Group and to the Deans. Microsoft Teams was the primary mode of communication between Information Services staff. Limited internet was restored by 2:52 p.m. and full restoration occurred at 6:08 p.m.

Approved: December 14, 2022

A debrief of the incident found many things went well and was a good full-scale test of the system. They include:

- Prompt response by personnel to stabilize the incident resulting in reduced damage.
- A timely and effective recovery process resulted in a partial, then full restoration of services in reasonable time frames.

However, it also identified many things that needed improvement. The primary areas included:

- Failure of proactively identifying critical infrastructure risks along with the implementation of prevention/mitigation strategies.
- Failure to quickly implement the emergency operations center (EOC).
- Lack of coordinated and timely communication.
- Lack of the ability to identify the impact to systems.

The debrief identified numerous areas for improvement, with the following ten to be included on the after-action improvement plan.

1. Pre-determine what systems are impacted by the various types of system outages. e.g. electrical, network, phone, and internet.
2. Identify an off-site EOC location that is independent of all university systems.
3. Evaluate the Amazon backup website to streamline its activation and evaluate whether the entire website should be moved to the cloud, such as the Amazon backup website.
4. Implement the use of Microsoft Teams as the standard communications platform for video conferencing, phone calls, chat and documents to support emergency operations, which will require the creation of the structure, training, and routine use of the tools.
5. Evaluate critical infrastructure for redundancy. e.g. alternative internet connectivity paths
6. Identify other reasonably foreseeable risks that can have significant impact to the university's operations. e.g. old pipes over servers
7. Evaluate alternatives to reduce risks to network critical infrastructure. e.g. utilize Springfield Underground to house servers.
8. Evaluate and prioritize the implementation of cellular signal boosters to support emergency operations/critical infrastructure.
9. Explore the utilization of FirstNet as a cellular carrier to provide priority cellular access during a major emergency/disaster.
10. Conduct an environmental assessment of data centers and other critical infrastructure locations.
11. Connect with the Emergency Managers of other local educational institutions and maintain up-to-date contacts.

Table of Contents

Incident Overview

10:48 a.m. to 11:10 a.m.

At 10:48 a.m. on Thursday, November 10, 2022, a 1" chilled water line for the HVAC system (see appendix) in the ceiling above the data center located in the Blair-Shannon residence hall ruptured, sending water into the northwest corner of the data center. This short circuited a smoke detector, activating the alarm. Within two minutes of the pipe rupture, telecommunications staff identified the leak and notified facilities management. At 10:53 a.m., the MOREnet internet service for the 417 area code failed. At 10:59 a.m., the leaking pipe was shut off. Facilities and Residence Life staff arrive on scene. By 11:02 a.m., Utilities Manager Ben Boslaugh and Rob Martin, Director, Cybersecurity and Enterprise Systems, were on scene. At 11:07 networking and telecommunications staff arrive on site and begin equipment damage assessment, followed by additional tarps being installed and water removal beginning.

11:11 a.m. to 11:35 a.m.

At 11:11 a.m., Chief Information Officer Jeff Coiner was notified. At 11:13 a.m., Director of Facilities Management Brad Kielhofner notified Vice President for Administrative Services Matt Morris, University of Space Management Jen Cox, Associate Director of Facilities Management Cole Pruitt, and Director of University Safety David Hall of the incident. Jen Cox notified Executive Vice President Zora Mulligan. At 11:24 a.m., Chief Information Officer Jeff Coiner called David Hall to discuss the impact and timeline of recovery. Associate Director of Information Services Theresa McCoy met with President Smart and at 11:32 a.m., she advised David Hall that President Smart requested a Missouri State Alert be sent to notify the campus. At 11:33 a.m., Jeff Coiner called President Smart to provide an update and discuss the broader notification of the issue and David Hall sent a text to Vice President for Marketing and Communications Suzanne Shaw and Director of Strategic Communications Andrea Mostyn with information on the incident for the Missouri State Alert that was being sent. However, the text went to Suzanne's office number rather than her cell, so she did not receive it.

11:35 a.m. to 1:00 p.m.

At 11:35 a.m., water removal from under the floor begins, verification of breaker panels and below floor circuits begin. At 11:36 a.m., Brad notified Matt, Jen, Cole and David that the Job Order Contractor was called in. At 11:45 a.m., the Missouri State Alert was sent. At 11:48, Andrea notified David the website was down and that Director of Web Strategy and Development Corey Canada was working on standing up the backup site. At 12:06 p.m., network and telecom staff began a group Teams/Zoom call to troubleshoot the connectivity issues and begin the equipment damage assessment. The fire suppression system is put into bypass to facilitate cutting and welding.

1:00 p.m. to 3:00 p.m.

At 1:26 p.m., ceiling tiles are brought over from another building and installed to help with cooling. At 1:36 p.m., Theresa McCoy and David Hall arrived at the site and received a briefing by Rob Martin and Steve Coffman. At 2:03 p.m., a text was sent out by David Hall updating the Policy Group of the briefing. It indicated that it could be 30 minutes or late tonight before service is restored if parts are needed from Columbia. It also indicated that some systems were still working and the outage was impacting other agencies. This was followed with an update to the Deans. At 2:28 p.m., requested MOREnet to point www.MissouriState.edu to www.MissouriStateAlerts.com and a second Missouri State Alert was sent

directing people to the backup site. At 2:32 p.m., Rob Martin texted the Policy Group indicating a piece of equipment was damaged. It was on the way from Columbia with an ETA of 5:00. He indicated they were trying to switch to an older piece to try to get some connectivity back up. At 2:52 p.m., MOREnet had partial internet service restored so the website redirect was canceled. At 2:59 p.m. Rob Martin texts an update to the Policy Group that it was partially restored.

3:01 p.m. to 7:02 p.m.

At 3:02, the deans were notified of the partial restoration of connectivity. At 5:57 p.m., MOREnet arrived with the parts and at 6:08 p.m., the internet to the 417 area was restored. At 6:15 p.m., Rob Martin texts the Policy Group to update them on the situation. At 6:55 p.m., this message was relayed to the deans. At 7:02 p.m., Matt Morris updated the Policy Group that the piping was repaired, and the building was being reheated.

Lessons Learned

The following group met on Wednesday, November 16, 2022, to debrief the incident and develop a process improvement plan:

Information Services
- Jeff Coiner
- Theresa McCoy
- Rob Martin
- Josh Stuppy
- Steve Coffman

Marketing and Communications
- Suzanne Shaw
- Andrea Mostyn
- Corey Canada

Administrative Services
- Matt Morris
- Brad Kielhofner
- Gary Chorn
- David Hall

A meeting of the Policy Group was held on Wednesday, December 14, 2022 to review and finalize the After Action Report. The group included:

- Clif Smart
- Ryan DeBoef
- Zora Mulligan
- John Jasinski
- Matt Morris
- Suzanne Shaw
- Dee Siscoe
- Rachael Dockery
- Jeff Coiner
- David Hall

What went well?

- Network and Telcom staff were in their office when the fire alarm activated. This allowed an immediate response to identify the issue was a water leaking onto the electronic equipment.
- Network and Telcom staff immediately made notifications for maintenance and began mitigation efforts to reduce additional issues.
- The response by Facilities Management personnel to stop the water flow was very quick.
- The response by Facilities Management and Residence Life custodial staff was very fast, which reduced the cleanup time.
- Having a Job Order Contract in place allowed for a team to immediately respond and begin repairs was effective.
- The overall cooperative relationships were very effective in coordinating repairs and recovery.

- Some systems were not impacted by the event, such as Microsoft Teams, Microsoft Office, Blackboard Connect (Missouri State Alert), texting, the campus phone system, and cellular connectivity.
- Preparation, such as having extra inventory on hand reduced the impact of the outage.

Overall, there was a prompt and coordinated response to the actual incident where everyone worked well together to bring it to a successful solution.

What could have gone better?

- The FM200 fire alarm system that is specific to the server room does not report centrally to dispatch. Had the incident occurred overnight or on a weekend, the leak could have gone undetected for an extended period of time.
- Not fully implementing the emergency operations plan at an early stage to bring the policy group together for briefings, decision-making and coordination. This led to several other items that did not go as well as it could have if the policy group, and potentially the broader emergency operations center (EOC) was convened.
- Having marketing and communications looped into the process early.
- Providing information across groups to allow others to know what actions they need to take.
- The lack of understanding how an outage would impact various systems, such as the Amazon redundancy website, Blackboard, etc.
- Students not knowing how they were to handle online courses, exams and assignments.
- The lack of contingency plans across campus for events such as this.
- Inconsistent communication to impacted partners.

The most significant issue revolved around communications. The emergency operations plan provides the structure and best practices to ensure communications are effective. This requires early recognition and activation.

What should be done differently?

These items are things to be considered for future incidents.

- Include marketing and communications in the original text messages for issues that come up.
- Send informational texts to the Policy Group early, even when it is uncertain of the scope of the impact to the University.
- Utilize the Administrative Services blog as a communications tool for employees.
- Request the activation of the emergency operations plan early for incidents that may be prolonged and impact more than one operational area.
- Everyone should feel comfortable recommending implementation of the emergency operations plan.
- Communicate to outside groups impacted by the emergency.
- Include the Chief Information Officer and the Chief Financial Officer to the Policy Group.
- Pre-determine what systems are impacted by the various types of system outages. e.g. electrical, network, phone, and internet.
- Identify an off-site EOC location that is independent of all university systems.

- Evaluate the Amazon backup website to streamline its activation and evaluate whether the entire website should be moved to the cloud, such as the Amazon backup website.
- Implement the use of Microsoft Teams as the standard communications platform for video conferencing, phone calls, chat and documents to support emergency operations, which will require the creation of the structure, training, and routine use of the tools.
- Evaluate critical infrastructure for redundancy. e.g. alternative internet connectivity paths.
- Identify other reasonably foreseeable risks that can have significant impact to the university's operations. e.g. old pipes over servers
- Evaluate alternatives to reduce risks to network critical infrastructure. e.g. utilize Springfield Underground to house servers.
- Evaluate and prioritize the implementation of cellular signal boosters to support emergency operations/critical infrastructure.
- Explore the utilization of FirstNet as a cellular carrier to provide priority cellular access during a major emergency/disaster.
- Conduct an environmental assessment of data centers and other critical infrastructure locations.
- Conduct early training for new staff members that are key to the University's emergency responses.

Many items were identified that will reduce the likelihood of future incidents and mitigate the consequences when they do occur. Some of the items that were identified are reminders to bake them into our processes, while others require follow-up action and are included in the improvement plan below.

Improvement Plan

1. Pre-determine what systems are impacted by the various types of system outages. e.g. electrical, network, phone, and internet.
    a. Assigned to: Jeff Coiner/Brad Kielhofner
    b. Completion date: January 31, 2023
2. Identify an off-site EOC location that is independent of all university systems.
    a. Assigned to: David Hall/Jimmy Stewart
    b. Completion date: January 31, 2023
3. Evaluate the Amazon backup website to streamline its activation and evaluate whether the entire website should be moved to the cloud, such as the Amazon backup website.
    a. Assigned to: Suzanne Shaw/Corey Canda/Jeff Coiner/Theresa McCoy/Rob Martin
    b. Completion date: January 31, 2023
4. Evaluate and prioritize the implementation of cellular signal boosters to support emergency operations/critical infrastructure.
    a. Assigned to: Steve Coffman
    b. Completion date: January 31, 2023
5. Explore the utilization of FirstNet as a cellular carrier to provide priority cellular access during a major emergency/disaster.
    a. Assigned to: Steve Coffman
    b. Completion date: January 31, 2023

6. Implement the use of Microsoft Teams as the standard communications platform for video conferencing, phone calls, chat and documents to support emergency operations, which will require the creation of the structure, training, and routine use of the tools.
    a. Assigned to: Jimmy Stewart/Theresa McCoy
    b. Completion date: March 31, 2023
7. Evaluate critical infrastructure for redundancy. e.g. alternative internet connectivity paths
    a. Assigned to: Jeff Coiner/Josh Stuppy/Brad Kielhofner/David Hall
    b. Completion date: March 31, 2023
8. Identify other reasonably foreseeable risks that can have significant impact to the university's operations. e.g. old pipes over servers
    a. Assigned to: Jeff Coiner/Rob Martin/Brad Kielhofner
    b. Completion date: March 31, 2023
9. Evaluate alternatives to reduce risks to network critical infrastructure. e.g. utilize Springfield Underground to house servers.
    a. Assigned to: Steve Coffman/Josh Stuppy/Rob Martin
    b. Completion date: March 31, 2023
10. Conduct an environmental assessment of data centers and other critical infrastructure locations.
    a. Assigned to: Steve Coffman/Rob Martin/Josh Stuppy/Brad Kielhofner/David Hall
    b. Completion date: March 31, 2023
11. Connect with the Emergency Managers of other local educational institutions and maintain up-to-date contacts.
    a. Assigned to: Jimmy Stewart/David Hall
    b. Completion date: March 31, 2023

The emergency preparedness manager will be responsible for monthly check-ins for each improvement plan item. The responsible individuals will provide a status update for their assigned tasks when requested by the emergency preparedness manager. This report recognizes that workloads and outside factors can impact the completion schedule, however, the dates are to ensure the tasks are completed as soon as reasonably practicable.

Summary

Every incident identifies the strengths and weaknesses of the university's ability to respond to emergency incidents that impact its operations. This specific incident tested many systems that are not typically tested in full scale. While some did not perform as expected, those failures had little to no impact on the outcome of the incident but did identify areas for improvement. The final chapter of whether this incident was a success or failure is whether the action plan results in meaningful improvements.

Appendix 1 - Photos

1” pipe that caused the leak. Note the hole in the pipe to the upper left of the valve. This pipe is original to the building, built in about 1965, and is in typical condition for the building.