

SUBJECT: BMIS472/694 Cybersecurity Class Project

Dear Missoula Education and Non-profit Leaders:

I teach a Cybersecurity class in the College of Business at the University of Montana called BMIS472/694 Cybersecurity Management Capstone. I've been working with LMG Security in Missoula to teach the students how to do a proper cybersecurity assessment and risk analysis for organizations. The final project for this semester is to have teams of three or four students work with an area non-profit, school, or small business to conduct a cybersecurity and risk assessment and make recommendations to improve cybersecurity. I need seven non-profits, schools, small businesses, or government entities this semester.

In the past, my students worked with the Downtown Missoula Partnership, Missoula Foodbank, Habitat Missoula, Confederated Salish & Kootenai Tribes IT group, Ecology Project International, Missoula Aging Services, CFAC, Missoula YMCA, Garden City Harvest, Aware-Inc, Montana High Tech Business Alliance, Missoula International School, Missoula Urban Development Project, Montana Natural History Center, Open Aid Alliance, United Way, Home Resources, CASA Missoula, Bright Ways Learning, Ravalli Aging Services, Missoula County IT, Families First, North Dakota IT, Run Wild Missoula, St. Josephs School, Wise River School, the Jeannette Rankin Peace Center, Missoula Homewood, Helena College, Mansfield Library, UM College of Business, Great Falls Schools, Columbia Falls Schools, Capsource.io, Missoula Chamber of Commerce, and CASA of Yellowstone County. I'm sure each of these organizations would be willing to visit with you about their experience. I've cc'd them on this message.

Here is a list of activities the students will be doing and the time commitment for your organization.

The students will do the following activities (The student teams can do the assessment remote via Zoom as long as there is someone from the organization that can consistently meet with them):

- 1) Review your appropriate plans & business documents.
- 2) Interview appropriate management, technical staff, and client serving staff.
- 3) Conduct a NIST cybersecurity assessment.
- 4) Conduct some technical vulnerability tests on your network (only if you agree to have these done).
- 5) Analyze the results of the NIST assessment (and vulnerability tests if done) to identify eight to ten risks.

- 6) Make recommendations on four to five key risks for how to improve cybersecurity in your organization.
- 7) Present their findings in a 30-minute presentation on May 1st or May 6th.
- 8) Provide a report that outlines the assessment, risks, findings, and recommendations.

The time commitment is as follows:

- 1) A few hours to gather business plans and documents.
- 2) A few hours for interviews with key management, technical, and client facing staff.
- 3) A few hours for vulnerability tests and scanning (only if you want this done).
- 4) A preliminary meeting on risks & findings.
- 5) A 30 minute presentation on May 7th. If that day doesn't work, we could do the presentation on April 28 or 30th.
- 6) Ten minutes to complete an online survey at the end telling me how you felt the students did on this cybersecurity consulting engagement.

Please let me know if you are interested in having a team of students do this cybersecurity and risk assessment for your organization. If you would like to visit with me about this project, feel free to call me on my cell 406-544-2246 or office 406-243-5985.

Take Care,

Dr. Shawn F. Clouse
Professor and Area Coordinator of MIS