CYBER WARRIOR CONSULTING

HOW DARTMOUTH BENEFITED FROM A PENETRATION TEST

JANUARY 2020

Cybersecurity threats are increasing, particularly for colleges with their mountains of personal and intellectual property data.

Dartmouth College, located in Hanover, NH, has 6700 undergraduate, graduate students and more than 4000 faculty and staff members across five schools and 50 departments, including business and medical schools.

A security audit recently conducted for Dartmouth identified the need for a penetration test. School IT executives determined that one hadn't been conducted for several years, so this one would be a good benchmark to gauge how well the institution was protecting itself. Dartmouth engaged CyberWarrior Consulting to conduct the penetration test in 2019.

The penetration test results provided several benefits to Dartmouth:

- It validated many prior actions to lower the risk of a cybersecurity breach.
- It identified areas for improvement that would further lower risk.
- It provided a reminder to all Dartmouth constituents, including trustees, that they must be mindful of how data is gathered and used.
- It strengthened the credibility of the Dartmouth IT department.

The penetration test results identified actions for detection, response, and recovery and other actions for Dartmouth's multi-year cybersecurity plan to lower risk and protect the institution.

CYBERWARRIOR

DO YOU INFORM YOUR STAFF OF AN UPCOMING PENETRATION TEST? MAYBE.

By Mitchel Davis and Sean McNamara
Dartmouth College.

Dartmouth College, Hanover, NH, is a large complex institution. We have 6700 students and 4000+ faculty and staff members across five schools and 50 departments, including business and medical schools.

DARTMOUTH

Cybersecurity is a top priority made challenging due to the open, sharing nature of high education institutions. In 2019, Dartmouth decided to conduct a penetration test for various reasons and selected CyberWarrior, a boutique cybersecurity consultancy, to conduct the test.

We thought long and hard about whether to tell the IT team in advance of the test. There are pro's and con's of doing so.

The pros for telling them in advance are:

- Allows staff to be prepared so they do not overreact.
- Helps the staff to respond to inquiries from the Dartmouth community during the testing process.

The cons for telling them in advance are:

- May mask problem areas such as patching or other processes not followed consistently.
- Can't learn the "real" situation of our protection regimen and gaps.
- Can weaken trust between team members and leaders.

CYBERWARRIOR

In the end, we chose not to tell the team in advance since we wanted to get an accurate picture of our cybersecurity program and be brutally honest with ourselves regarding gaps or weaknesses.

Further, we believe no-one can know everything about cybersecurity, therefore we wanted to use the test as a learning experience and asked the staff to do the same.

We repeatedly told the staff that we weren't looking for scapegoats or seeking retribution for any gaps or weaknesses. We continually stressed that we are a team that continually learns and improves together.

While there were some "bumps" to overcome with certain staff members, overall, we believe we took the right approach for Dartmouth to get the most from the penetration test.