POTENTIAL QEP THEME: CYBER CITIZENRY

Abstract:

One of the more effective ways to define Cyber Citizenry is by analogy. Like computing, driving can be extraordinarily beneficial and extremely dangerous. We spend years modeling both driving and vehicular maintenance behavior for children before sending them off to driver education, followed by an apprenticeship with a learner's permit before allowing them to join us on the highways as licensed drivers who respect the rules, responsibilities and etiquette of sharing the road. Unfortunately, the same is not true for our introduction to cyber infrastructure and cyber behavior. Despite the best efforts of computer security professionals, all it takes is one user clicking on the wrong link or downloading the wrong file and the entire cyber infrastructure of an organization can be at risk. Even simple little things like forwarding an e-mail Christmas card can bring the computing power of an organization to a halt if the file is too large or contains a virus. Further, hard to detect activities such as indulging in piracy (e.g., downloading illegally obtained movies) make an organization vulnerable to legal risks and may foster an environment where unethical behavior runs rampant. It is ironic that every faculty and staff member at Radford University is required to take online cyber security training every year, but our students are not exposed to the same topics. Radford University graduates should enter the world beyond equipped to be good Cyber Citizens by being able to recognize and avoid risky cyber behaviors, by understanding and practicing safe, ethical and productive cyber behaviors, and by being aware enough of how cyber infrastructure works to understand their role in it and to adapt to and adopt technologies that emerge in their lifetimes.

Overview of Theme:

Radford University graduates should be equipped to be good Cyber Citizens by being able to recognize and avoid risky cyber behaviors, by understanding and practicing safe, ethical and productive cyber behaviors, and by being aware enough of how cyber infrastructure works to understand their role in it and to adapt to and adopt new technologies that emerge in their lifetimes.

Current Status of Theme at RU:

The current Radford University Core Curriculum does not provide sufficient awareness of cyber infrastructure or cyber security. Outcomes of University Core A include an ability to explain how digital information is organized and communicated and to identify ethical and other considerations for using digital information. These outcomes provide a minimal foundation for using technology, but they do not provide graduates the knowledge and skills needed for effective cyber citizenship.

Ways Adoption of this Theme Might Move RU Forward:

We propose a hub and spoke model that has the potential to make RU a national leader in preparing graduates for the rapidly changing cyber world. The hub consists of a core set of cyber citizenry topics

required of every student. A task force would be put together made up of IT faculty, other interested faculty, ITR staff, and corporate partners to identify this core set of topics. This task force would also seek input in the cyber security and cyber citizenry guidelines published by the Department of Justice, Department of Education, Association for Computing Machinery and others. The spokes are program-based: each academic program would identify and deliver a set of cyber infrastructure topics specific to their discipline. For example, beyond the core set of topics, the cyber background required for an Elementary Education major might differ significantly from that required for an Accounting major.

Who Might be Involved in Implementation of this Theme:

Faculty in every program on campus could be involved in this theme, as well as corporate partners and ITR staff.

Benefits for RU Students Resulting from the Adoption of this Theme:

Through the implementation of this theme, RU has the potential to better prepare our graduates for the cyber world beyond their undergraduate education. In addition, as the cyber reputation of our graduates grows, this could give them a competitive advantage in internships and job placement as well as throughout their careers.