CEHC 242 – Cyber Security

Instructor: Bryan L Haynes, MPA, CISSP

Office Hours
By appointment via Phone

Course Summary:

Our world is more connected today than it has ever been in our history. Tomorrow we will be
more connected than we are at this very moment. While each connection we make in the
virtual world is intended to make our lives easier, we must ask ourselves, “What if someone
pulled the plug? How do we respond? Should we have been able to prevent it?”

Since the creation of electronic devices that transmit information there have been criminals,
terrorists, and nation states that seek to exploit them for financial, social, or
political/ideological gain. This threat has become one of the top national security priorities,
requiring a cyber force that includes the training of people who don’t even work as cyber
professionals. Maybe you have seen the signs in your current work places, “Security is
everyone’s responsibility.” A simple statement has never been truer.

This class is intended to paint a broad brush of the cyber security landscape and introduce you
to the many aspects of how cyber security is viewed by industry, private sector business, civil
government, military, and academia. The class will also provide a cursory overview of technical
knowledge of the underlying systems used to implement cyber security.

Students taking this class will be well equipped to take more advanced technical courses in a
multitude of disciplines that make up cyber security. It will also provide the more technically
advanced students an opportunity to better understand the management, policy, and political
equities involved in cyber security from a mid-micro to macro organizational level.

Most of the interaction between cyber security experts and the clients they serve is conducted
via video teleconference. So it is fitting that this course is being offered online. As a class we will
work to operate in a professional format that in most cases mimics real world situations. This
will be the best way to bring the real world into our virtual classroom.

Below you will find a weekly break down of assignments and topics to be covered as well as
what are required of you each week. Each week is annotated with a “pre-record” or “live” tag.
If it is a pre-record please feel free to watch or listen to lectures at your leisure. If it is a live
discussion it is highly encouraged that you log in and participate. If a live discussion is canceled,
it will be replaced with a pre-recorded lecture on the same topic, or a pre-recorded lecture
from a new topic will take its place. If a live discussion is canceled and there is an assignment due that day, you must still complete the assignment.

There will be a total of four live sessions all held on Wednesdays which are highlighted in bold on the class schedule.

**Learning Goals:**

- Better articulate the challenges of Cyber Security in an organization
- Understand how the 20 Critical Controls can be applied
- Identify good and bad Cyber Security policy
- Understand the various types of cyber attacks
- Determine the difference between security devices and products
- Articulate the difference between types of policies

**Assignments:**

**Weekly Cyber/Cyber Security News Article** – On specified weeks, each student will seek out a specific news article related to cyber security to post. With the post, each student should write a half page analysis of why this article is important. What are the impacts to a particular industry, demographic, region, etc? This is not a summary, use your analytical skills.

**Weekly Discussion** – Every week students will be required to post a response to the discussion question as well as respond to 2 comments on a classmates discussion thread. Comments should be no less than one paragraph in length. The topic will relate to that week’s subject area. Students are encouraged to engage each other in discussions that further analytical and creative ideas. Discussion close on Friday at midnight.

**Written Assignments** – There are various written assignments that range from research paper, power point presentation, or free choice. See assignments in the weekly module for more details.

**Final Project** – The Final Project will be announced around the mid-term.

**Grades:**

- Participation: 30%
- Written Assignments: 30%
- Final Project: 40%

**Grading policy**
Timelines for assignments and project will be outlined in Blackboard or stated by me via a course announcement. Late assignments and project submissions will be downgraded unless in special cases cleared with the instructor first. Handing in something is better than nothing!

**Cyber Readings and Resources**

**Required Text Books**


**Required Online**

DHS Cyber Security Blueprint
http://www.dhs.gov/blueprint-secure-cyber-future

NIST Publications

OMB Publications
http://www.whitehouse.gov/omb/circulars_index-info/

FISMA

HSPD-12
http://www.idmanagement.gov/


**Students with Disabilities**

If you have a disability and anticipate needing accommodations in this course, please contact me to set up a meeting within the first two weeks of the semester or as soon as you become aware of your need. The Director of Disability Resource Center is located at Campus Center 137 and can be reached by phone at 442-5490.
Academic Honesty

You are strongly encouraged to find the balance between consulting with your fellow students on course concepts while handing in your own work when you turn in assignments. Make sure you properly cite and document and sources when you have borrowed ideas or language (including code and scripts).

Responsible Use of Information Technology

Students are required to read the University at Albany Policy for the Responsible Use of Information Technology available at the ITS Web Site: https://wiki.albany.edu/display/public/askit/Responsible+Use+of+Information+Technology+Policy