Course Prerequisites:
CIS 2010; CSP 1, 6.7.

Primary Text:

Readings:
Clark, Richard (2009), War in Cyberspace, National Interest, Nov/Dec, pp. 31-36.

Optional Material
Free! Windows 8 Professional available through the CIS Department's involvement with Microsoft's Developer Network's Academic Alliance program. The student software program is called Dreamspark. developer's catalog is available free to any student who is taking a CIS Department class. This includes products such as MS Windows 8, SQL Server, Visual Studio.Net 2010, MS Project, Visio, etc., etc., et Make use of it as much or as little as you like. These are the full-blown products, not cut-down student versions. Use of the Microsoft corporate jet is NOT included as part of this deal! Use this link for access.

Anonymous Feedback
Give me any type of feedback you want. Try to be constructive. I've created a gmail account which any of my students may login and send me an anonymous email. The userid is: "mcdonaldfeedback" (no (all lower case - no quotes): improvemycourse.

Catalog Description
This course provides a strategic exploration into the prevention and response to intentional abuse of business information systems. This abuse frequently leads to diversion of resources, interruptions of systems that develops into a variety of losses that can seriously impair an organization's performance. Students will be prepared to plan and manage organizational incident and forensic preparedness, including information controls, information practices, incident response plans, forensic techniques, and forensic analysis.
readiness, and preservation of evidence in the form of electronically stored information. The course includes experiments in the investigation of organizational policy violations

**Detailed Course Objectives**

Through successful completion of this course, students will develop abilities to

1. Explain the organizational relationship between activities directed toward policy enforcement, computer forensics, data recovery, incident response, and privacy protection.
2. Plan strategies for information systems control governance and policy enforcement.
3. Plan strategies for organizational readiness for computer incident response such that collection, preservation, presentation and preparation of computer-based evidence will optimally support business continuity, criminal law enforcement and civil litigation.
4. Create and evaluate organizational information services policies for incident response and business continuity.
5. Evaluate at both strategic and technical levels the organization’s computer incident response systems, architecture, and staff capabilities.
6. Plan, organize, and manage an organization’s computer incident response processes and computer forensics investigation processes.
7. Explain the ethical, technical and economic rationale for specific organization information systems incident response and forensic capabilities.
8. Detect typical forms of computer crime and abuse and recognize/preserve the relevant evidence.

**Exams**

Make-up exams are NOT given. Students missing an exam will receive a zero on that assignment. Exams may be taken early if the instructor is given a legitimate reason (religious holiday, pregnancy, etc.).

**Lab assignments**

The course will include lab assignments to be completed by individual students either during class or outside of class. The lab assignments are based on Virtual Machines running En during class or by remote access outside of class. Remote access times are sometimes shared with other forensics students, and may only be available during certain assigned time.

Study Center is located on the 9th floor of the RCB Building, and has additional workstations available on a first-come, first-served basis.

**Discussions**

The course will include in-class discussions of the topics outlined in the schedule. These discussions include three cases: (1) Omega Engineering, (2) iPremier, and (3) Sue.

Students will have individual opportunities to contribute thoughtful and critical oral observations during class discussions focused on the course objectives. There will be readings assign meetings. Students will have opportunities during the semester to introduce and comment on these readings during in-class discussions. Outside of class meeting times, there will also be course-related discussions online using an email group server, wiki pages, and/or online social networking.

**Team Activities**

Some course activities will be organized as teamwork. These include: (1) RollingCat case, and (2) The testimony tournament. Assessment of performance in the Rollin

The testimony tournament assessment is generally based on the ability of individual students to sustain challenges to the quality of the knowledge developed by their team of the RollingCat case. This activity will be competitive, and “bonus” credit may be awarded to winning teams. These activities are further described in the activity de advance of the activities. Students will form self-managing teams for the purpose of completing team activities. Each team is expected to persist through the course. Peer the overall grading/evaluation of individual performance. Consensus on the relative contributions of each of the team members will be derived through assessment of individual performance, and evaluation of team processes. Unless team members inform the instructor in writing to the contrary, the assumption will be that each contributed equally to the assessed products of the team.

**Richard Clark "War in Cyberspace" article analysis (article available from list above on this page)**

Each team will prepare one or more MS Word (Space 1.5 spacing, 11 point type, Times Roman) and upload it to the appropriate D2L dropbox.

The page(s) must first demonstrate the team’s understanding of the issues presented by Clark. Second, the team
must analyze the current public and private sector attitudes toward cyber d supportable opinion based on facts, as to why the United States is either vulnerable or well-prepared to fend-off a cyber attack in the near future. The teams’ students ability to research a te solutions, analyze data, synthesize data from different sources, and to compare and to evaluate distinct solution technologies with a clear train of fact-based argumentation. Any and all con stated. To insure research originality, students are strongly encouraged to seek information beyond web pages, and from at least one original source NOT already cited in the article.. citations and full references to all direct sources.

Class Presentation

Each team will prepare a brief (e.g. ten-minute) in class presentation of their opinion as to the future of cyberspace warfare capabilities of the United States. Each presentation will be followed by an open question and discussion session by the class.