The Epic Challenge
The Threat Within
“Syllabus”

Spring 2017

University at Albany, SUNY
The Epic Challenge
The Threat Within

Course Description

The Epic Challenge: “The Threat Within” - A new operating reality is confronting public and private sector organizations and institutions of all shapes and sizes everywhere: the threat from within that is able to exploit and expose an organization’s greatest competitive edge – the “secret sauce.” Initially many experts thought of the insider threat challenge as a technical problem to solve. However, if there is anything that one of the largest and most damaging data breaches in U.S. Government history – Edward Snowden – has taught us, it is that this challenge is simply not one dimensional. Insider threats can surface at the strategic, operational and tactical layers of an organization, and therefore, the solution needs to be comprehensive, logical, and balanced.

In this course, students from a variety of disciplines will become “cyberinterns” and work in teams with course faculty, graduate assistants, and industry experts as mentors using an online/cloud communication platform known as iQ4. The goal of the course is to enable students to analyze realistic case scenarios and identify the depth and breadth of the cybersecurity challenge from multiple perspectives. Students will focus on the interrelated dimensions of the threat (which may include but are not limited to technical, procedural, legal, behavioral, skills/proficiencies) and the spectrum of constituent cyber domains/functional areas in which to identify solutions.

Industry Motivation: Tackling Skills Shortages - Cybersecurity Financial Services and Healthcare firms report a significant shortage of graduates with the skills, experience and an understanding of financial markets and technologies, in critical infrastructure including Cybersecurity, Business Resiliency, IT Risk, Business Risk and Auditing. In response to these ‘skill–gaps’, iQ4 has launched the Cybersecurity Workforce Alliance (CWA) to meet present and future industry demand for Cybersecurity talent, and producing graduates that are “workforce ready” … our next-generation workforce. Mission: Improve the cyber security skills and scale the college student workforce, so they are more attractive to hire and can provide almost immediate value to the public & private sector by improving a company’s Cybersecurity capabilities. Frank Cicic - CEO/Founder iQ4.

Student Motivation: Increased workforce readiness from a virtual-internship mentored by industry experts has proven that the CWA course increases the chances of physical internships and jobs. This is a 3-credit course. The content for the CWA challenge covers core competencies e.g., knowledge, skills, and abilities relating to the identification, detection, protection against, response to, and recovery from an insider threat including how to build and maintain communications with executives, peers and regulators. And essential skills (e.g., teamwork and communications skills), which are required in the workforce. The assignments of the virtual internship are designed to assess both core competencies and essential (soft/professional) skills.

Students Gain:
Communication experience
- Knowledge and practice in producing executive briefing material/memos
- Knowledge and practice in producing Infographics
- Knowledge and practice in producing succinct briefing videos on the current situation, the derived problems and implications and what actions are being taken to mitigate, respond or defend against future incidents.
- Presentation skills to a large audience of employers, mentors, academics/educators and government attendees at the “finals’ (both individual role participation and the team based approach to the “Threat Within” challenge).
- A crash course in networking prior to the finals presentation
**Intellectual Skills developed - the abilities required to process the subject matter**
Professionalism, critical thinking, problem solving, advocacy, communication, teamwork, written communications, verbal communications, innovation and creativity, confidence, composure, poise, coalition building, supervision, leadership, analytics, ability to pivot/change, decision making, contextual awareness, business writing skills (as opposed to academic writing).

**Professional/practical skills – those skills specific to a subject area**
Contextual awareness and knowledge of Cyber security threat landscapes, actors and frameworks used by employers to protect, defend and respond to Cyber, risk and compliance challenges. Understanding of job roles within industry/employers and why they are needed and have different skill sets, yet are essential to form a composite capability.

**Prerequisite:** Sophomore, junior, or senior standing.

**Strategy**
The [ultimate] goal is to enable you, the student, to get creative and dissect a scenario in identifying the depth and breadth of the challenge, generating excitement and interest in the area of cyber-security from multiple disciplines. In other words, based on your perspective, you will focus on the interrelated dimensions (may include but not limited to; technical, procedural, legal, behavioral, skills/proficiencies) and the spectrum of constituent cyber domains/functional areas to identify solution(s).

**Instructors**
Dr. Ian M. MacDonald (imacdonald2@albany.edu), instructor  
Dr. Hadi Salavitabar (hsalavitabar@albany.edu), instructor  
Chathura Wickramamge (cwickramage@albany.edu), head teaching assistant  
Kirstin O’Sullivan (kosullivan2@albany.edu), teaching assistant  
James Vital (jvital@albany.edu), teaching assistant  
Jonathan Eustache (jeustache@albany.edu), teaching assistant  
Brendan Jones (bfjones@albany.edu), teaching assistant

Note: All teaching assistants will have scheduled office hours and assist with Friday mentor sessions. Please check Blackboard and/or iQ4.com for details.

**Course Contact Hours**
This course is offered in a hybrid-online format. Approximately 50% of the course will be conducted online through the iQ4 platform. The course meets in-person for 75 minutes per week. Additionally, you will be meeting with your team both online and in-person for several hours each week to work through each assignment.

**Textbooks**
There are no required printed textbooks for this course. However, there are several required readings which will be available through the online iQ4 platform.
Course Goals

Utilizing the National Institute of Standards and Technology (NIST) Cybersecurity Framework, provide a mitigation and management strategy for the scenario provided, covering each of the following areas:

- Identify
- Detect
- Protect
- Respond
- Recover

Course Learning Objectives

1. Recognize and define insider threat as it applies to the financial sector
2. Identify the constraints and decision criteria
3. Identify alternative methodologies and actions
4. Evaluate the alternatives
5. Choose the best solution
6. Formulate and present your solution

Academic Honesty

For individual assignments, you are expected to do your own work. For team assignments, you are expected to make a unique contribution, properly citing sources and avoiding misconduct, such as plagiarism, at all cost. All violations of academic integrity will be reported to the university and proper protocols will be followed with respect to academic dishonesty.
Case Studies

The following four (4) case studies are provided to give you an understanding of the complexities involved with insider threats. Your team must pick one of the case studies to follow throughout the project.

Case Study 1: Fraud

A lead software developer at a prominent financial services firm devised a scheme by which he could earn fraudulent rewards points by linking his personal accounts to corporate business credit card accounts of third-party companies. He cashed in the rewards points for gift cards and sold them in online auctions for cash. In all, he was able to accumulate approximately 46 million rewards points, $300,000 of which he converted into cash.

Case Study 2: IT Sabotage

The firm employed a contractor as a night time security guard who was extensively involved with the cyber underground and the leader of a hacking group. He used his security key to obtain physical access to the computer that controlled the heating, ventilation, and air conditioning (HVAC) for the firm using various methods, including password-cracking programs and a botnet, he rendered the HVAC system unstable, eventually leading to a four-hour outage during trading time. The insider and his cyber conspirators were planning to use the firm’s systems to conduct a distributed-denial-of-service (DDOS) attack against unknown targets.

Case Study 3: Theft of Intellectual Property

China sought to develop a next generation trading platform for brokers and dealers. China’s state-owned Pangang conspired to steal the technology (design and code) developed by the US financial services company. A contractor (development manager) who had spent 15 years with that US Company used privileged position to help Pangang. The financial impact of this incident is estimated to be in the billions of dollars, and that does not factor in the consequent loss of competitive advantage for the firm.

Case Study 4: Espionage

A former senior financial analyst was arrested as he was boarding a flight for Switzerland carrying a large amount of sensitive customer data of high profile clients. Computers searched in his home led to the discovery of emails offering to sell secrets to Syria and China. He is thought to have been motivated not only by money (he had very heavy personal debts), but also by a sense of disgruntlement, as he complained frequently to former coworkers and neighbors about his job.
Scenario

Overview

Goliath National Bank (GNB) has developed and tested an electronic-trading system over the past 2 years, investing approximately $30 million in the people, processes, and technologies to support a state-of-the-art e-trading system and challenge market leaders.

Recently, key components of GNB’s trading algorithms have surfaced on the dark web. A GNB employee is suspected, but it’s unknown how the infrastructure or data were compromised. In addition, the security operations center has disseminated several reports over the past few months indicating the financial industry is being targeted by sophisticated threat actors capable of employing blended attacks, including exploiting technical vulnerabilities and human intelligence sources.

Senior management has identified the e-trading system as critical to the future of GNB and expressed concerns that the e-trading system has created opaque risk to the firm.

GNB Profile

<table>
<thead>
<tr>
<th>Industry:</th>
<th>Financial Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Headquarters:</td>
<td>New York, NY</td>
</tr>
<tr>
<td>Size:</td>
<td>50,000 employees (not including subsidiaries, affiliates, or joint ventures)</td>
</tr>
<tr>
<td>Scale:</td>
<td>Global, operating in 90+ countries across Americas, APAC, EMEA and LATAM either directly or indirectly (via subsidiaries, affiliates or joint ventures)</td>
</tr>
</tbody>
</table>

Scope of attack: What happened: The suspected individual moved from a role within the IT organization within the Singapore office to the subsidiary to lead the development and integration of the help desk function. The suspected insider printed large amounts of sensitive and confidential data over a 6-month period that the individual already had access to prior to moving into the new role. She then mailed the large volume of printed documents to a foreign embassy.

Which embassy: irrelevant – feel free to assume any embassy you wish

Discovery?: an anonymous tip by an internal employee who knows the suspected insider was sent to the Security Operations Center

Why/How?: not known yet – assume there is a behavioral element

GNB network topology:
Mission

GNB’s Information Risk Management teams will conduct a full risk assessment of the e-trading system. Information Risk Management teams consist of five functional groups across GNB, including Information Risk Officers, Behavioral Analysts, Cyber Threat Analysts, Compliance Analysts, and IT Risk Analysts. Groups will work together to conduct research, gather information, and leverage resources effectively to provide critical input and support individual team requirements.

Risk assessments will identify the most critical people, processes, and technologies at GNB and help senior management make critical business decisions to appropriately manage risk at the firm. Identifying vulnerabilities, detecting current threats, protecting against threats, responding to compromises, and recovering operations is fundamental to sound IT Risk management.

Information Risk Management teams will provide senior management with a full risk assessment of the e-trading system and present a comprehensive insider threat management program leveraging industry guidance and best practices.
Project Role Profiles

During the semester-long team project, you will have a chance to play one of the following critical roles:

**Behavioral Analyst, Junior**

Demonstrates ability to understand human behavior involved in threat scenarios and is adept at applying psychological attributes that suggest vulnerabilities to an organization’s people, processes, and technologies. Maintains an ability to analyze intruder exploit tools, identify and document the impact of resulting attacks and provide insight to team members based on such findings.

**IT Risk Analyst, Junior**

Demonstrates a basic understanding of information technology risk analysis. Understands the effects of various types of risks, such as potentially widespread Internet attacks, national security issues as they relate to their physical threats, financial threats, loss of business, reputation or customer confidence, and damage or loss of data.

**Compliance Analyst, Junior**

Communicates well with other team members with various levels of technical understanding in a written and oral manner. Demonstrates an ability to design, document and communicate policies and procedures, navigate through the organization and maintains diplomacy in highlighting any potential breaches.

**Cyber Threat Analyst, Junior**

Demonstrates clear understanding of baseline skills needed to understand how systems and software are configured, how they work, how the risks associated with various technologies in use and the strategies and technical recourse for a potential breach in systems. Practical knowledge of network protocols, malicious code, programming, and incident handling skills.

**Information Security Officer, Junior**

Manages information security implications within an organization, specific program, or other area of responsibility, to include strategic, operational, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.

**Team Role**

Your team can choose one of the following options for how you will view the preparation of project materials:

- **Option 1**: Your entire team is employed by GNB
- **Option 2**: Your team is a consulting firm hired by GNB
### Schedule of Topics

**Please Note:** Please check iQ4 frequently for the most current schedule. Note that the “Tech Track Mini-Lesson” activities will be determined during the semester and posted on iQ4.com.

<table>
<thead>
<tr>
<th>Week of</th>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/23 – 01/27</td>
<td>Course Introduction, iQ4 Platform Tutorial, Creating Your Passport</td>
</tr>
<tr>
<td>01/30 – 02/03</td>
<td>Cyber 101 – Part 1: What is Cybersecurity? What is “The Threat Within”?</td>
</tr>
<tr>
<td>02/06 – 02/10</td>
<td>Cyber 101 – Part 2: Governance, Risk and Compliance, NIST Framework</td>
</tr>
<tr>
<td>02/13 – 02/17</td>
<td>Cyber 101 – Part 3: Exploring Role Profiles in Cybersecurity</td>
</tr>
<tr>
<td>02/20 – 02/24</td>
<td>Designing an Insider Threat Program for the Financial Sector</td>
</tr>
<tr>
<td>02/27 – 03/03</td>
<td>Assessing the Efficacy of an Insider Threat Program</td>
</tr>
<tr>
<td></td>
<td>Tech Track Mini-Lesson 1: Certified Network Defender Module</td>
</tr>
<tr>
<td>03/06 – 03/10</td>
<td>Identify</td>
</tr>
<tr>
<td></td>
<td>Tech Track Mini-Lesson 2: Computer Hacking Forensics Investigator Module</td>
</tr>
<tr>
<td>03/13 – 03/17</td>
<td>NO CLASSES – Spring Break</td>
</tr>
<tr>
<td>03/20 – 03/24</td>
<td>Protect</td>
</tr>
<tr>
<td></td>
<td>Tech Track Mini-Lesson 3: Certified Ethical Hacker Module</td>
</tr>
<tr>
<td>03/27 – 03/31</td>
<td>Detect</td>
</tr>
<tr>
<td></td>
<td>Tech Track Mini-Lesson 4: Tool Demo (RedOwl)</td>
</tr>
<tr>
<td>04/03 – 04/07</td>
<td>Respond</td>
</tr>
<tr>
<td></td>
<td>Tech Track Mini-Lesson 5: Tool Demo (RedOwl)</td>
</tr>
<tr>
<td>04/10 – 04/14</td>
<td>Recovery</td>
</tr>
<tr>
<td>04/17 – 04/21</td>
<td>Team Building, Team Final Presentation Preparation</td>
</tr>
<tr>
<td>04/24 – 04/28</td>
<td>Final Presentation Preparation – Combined Team</td>
</tr>
<tr>
<td>05/01 – 05/05</td>
<td>Final Presentation Preparation – Combined Team</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Last week of mentor sessions</td>
</tr>
<tr>
<td>05/08 – 05/12</td>
<td>Final Presentation at the Federal Reserve Bank in NYC</td>
</tr>
<tr>
<td></td>
<td>Thursday, May 11, 2017 – check iQ4 for detailed itinerary</td>
</tr>
</tbody>
</table>
Assessment

Team Assignments

You will be working on a team consisting of 5 – 10 peers, each taking on one of the given role profiles (see “Project Role Profiles”). Once your team has been formed, you will have weekly deliverables in the form of documents, infographics, and videos, as well a weekly contribution to the mentored Q&A sessions.

No later than 48 hours before each mentor session, you will be required to post your completed assignment, along with a 2-minute video overview of your work for that week to the iQ4 platform. Prior to the mentoring session, industry and faculty mentors will watch your video and review all documentation relevant for that week’s assignment. During the mentor session, you will be given feedback from the mentors and have the opportunity to ask questions and seek clarification for the current and future assignment. Mentors will provide guidance on how they would tackle the real-world assignments in their own organizations so that you have a framework to build on. Failure to submit an individual or team-based assignment element, e.g. executive report, Infographic or video will negatively impact your project grade for that week.

Individual Assignments

There will be approximately ten (10) individual “mini-assignments” given throughout the semester. These assignments simply verify that you have read and understand the main points from the assigned reading for each week. The format of the assignments will be short-answer. Completing these assignments should not take more than 15 – 20 minutes. Mini-assignments will be typed and submitted online through the iQ4 platform.

Participation

You are required to attend every mentor session, unless you have a documented excuse. Attendance will be taken at the beginning of the session. If you are profoundly late, you will be marked as absent.

Additionally, you are expected to contribute weekly to discussions and threads on the iQ4 platform. We will track the number of posts, responses, questions, etc. that you post to the platform. You are required to make at least one (1) significant contribution to a discussion each and every week.

Grading

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual Assignments</td>
<td>20%</td>
</tr>
<tr>
<td>Participation (Attendance &amp; Platform Activity)</td>
<td>20%</td>
</tr>
<tr>
<td>Team Projects</td>
<td>50%</td>
</tr>
<tr>
<td>Final Presentation</td>
<td>10%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

Letter-Grade Assignment:
A (92-100), A- (90-91), B+(88-89), B (82-87), B- (80-81), C+ (78-79), C (70-77), D (60 - 69), F (<60)