The Threat Within
Epic Challenge

Course Outline

Course Description

In this **Epic Challenge**, students from a variety of disciplines become “cyber-interns” and work in teams on cybersecurity cases associated with insider threats (fraud, sabotage, espionage, theft of intellectual property). Students work with course faculty, student peers, and industry experts as mentors using the iQ4 applied learning platform. Student working on the cybersecurity cases have different job role (ex. Information Security Officer, Information Technology Risk Analyst, Behavioral Analyst, Compliance Analyst, Cyber Threat Analyst). The course covers core competencies (knowledge, skills, and abilities) and utilizing the National Institute of Standards and Technology (NIST) Cybersecurity Framework, students provide a mitigation and management strategy for the cybersecurity cases covering 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. A Department of Homeland Security table-top exercise methodology is also used to identify findings and recommendations. The course also strengthens essential soft skills, such as teamwork, critical thinking, and communications, which are required in the workforce. The assignments in this course are designed to assess both core competencies and soft skills.

Learning Outcomes

Upon completion of the course, students acquire the following:

*P**ractical Skills*** - Contextual awareness and knowledge of cyber security threat landscapes, actors and frameworks used by employers to protect, defend and respond to cyber-attacks.

Communication Skills - Knowledge and practice in producing written reports and succinct executive presentations on the current situation, the derived problems and implications and what actions should be taken to mitigate, respond or defend against future incidents, both individual role participation and team-based approach to the “Threat Within” challenge, and a crash course in networking prior to the final presentation.

Strategy Skills - 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.

Course Delivery, Format, & Grading

Course Delivery

This course is offered in an online-blended learning format. All of the lecture materials and assignments will be available on the iQ4 Platform. The course schedule will be distributed to students at time of registration. Students work in teams (cohorts) during the course meeting time throughout the term (four weeks).

Each cohort of students will be broken into teams. The teams will complete assignments in-class on a weekly basis, based on one of the case studies outlined within the syllabus which will also include a final presentation.

There are two (2) individual assignments that are submitted to the iQ4 platform.

Every week will have mentor interaction.

The course will progress as follows:

1. Introduction / Cybersecurity One-on-One [Week 1]
2. The NIST Framework Case Studies [Weeks 2 - 3]
3. Final Presentation [Week 4]

Textbooks/The iQ4 Platform

There are no required printed textbooks for this course. Resources assignments will be available on the iQ4 platform, especially given the rapid-moving nature of Cybersecurity, students and teams will need to supplement the provided materials with online research. The iQ4 platform also includes discussion boards where students, instructors and mentors post questions and general discussions regarding Cybersecurity events.

In addition, the iQ4 platform provides each student with a digital passport that is used to provide a digital transcript evidencing successful completion of the course, an inventory of each student's knowledge, skills and abilities, and to help students identify career pathways.

Session Format

Each session will be broken into two discrete parts – The Lesson portion and the Assignment portion.

The Lesson Portion - Typically, each session's start-up will be based on the Lesson material for that week which will lead into to a discussion on the day's team assignment.

The Assignment Portion - In each session, teams are required to deliver a 10-minute presentation using PowerPoint to the mentors based on the Assignment for that day. This presentation will then form the basis for discussion with the mentors and will also contribute to the student grades.

The instructor will be available for student consultation via phone and Zoom video conferencing during announced office hours and by appointment.

Case Study

The following five (5) case studies are provided to give you an understanding of the complexities involved with insider threats. Your team will use one of the case studies to follow throughout the course.

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.

Case Study 5: Information Technology Sabotage At your financial institution you just received a panicked call from one of your system administrators detailing that your organization has been hit by ransomware. This ransomware seems to have infected and then encrypted all the data, including backups, of two of your servers. According to the ransom you received,

you must pay the ransom in a week or the encryption key will be deleted and the data lost forever. The work week is bustling and people are starting to ask why the servers are down.

Project Role Profiles

Each student will have an opportunity to perform one of the following roles:

Behavioral Analyst*:* 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: 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*:* 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*:* 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*:* 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.

Course Grading

10% Individual Assignments
30% Platform and Discussion Board Participation
30% Team Assignments
30% Final Presentation
100% Total

Cyber Crimes

Epic Challenge

Course Outline

Course Description

In this **Epic Challenge**, students become "cyber interns" and work in teams with course faculty and industry experts as mentors using the iQ4 applied learning platform. The goal of the course is to enable students to analyze cyber-crime cases in fraud, theft, assault, terrorism, extortion/espionage, and trafficking and identify the depth and breadth of cybersecurity from multiple perspectives. Students will focus on different types of cyber threats to include: data breaches, ransomware and illicit traffic and have different job roles (ex. Cyber Security Attorney, Security Operations Center Manager, Law Enforcement with Specialization in Cyber Crime / Digital Forensics, Insurance Investigator Negotiators (Ransomware / Extortion), Chief Financial Officer, Threat Actor). The content of the course covers student core competencies (knowledge, skills, and abilities) relating to the case scenarios studied. Action plans are prepared to reduce risk and remediate the cyber-attacks that occurred. The course also strengthens essential soft skills, such as teamwork, critical thinking, and communications, which are required in the workforce. The assignments in this course are designed to assess both core competencies and soft skills.

Learning Outcomes

Practical Skills

The course format requires that students operate as project teams addressing challenging scenarios within a case study and/or scenarios involving a fictional company addressing an advanced, persistent web-based threat. Students will conduct online research to assist with addressing the challenges posed by the current landscape and rapidly evolving, emerging technologies. Students will also develop their project management skills. The assignments are project team based and will require students to define responsibilities to ensure fair distribution of the workload and will need to plan their weekly activities to meet the deadlines. Specific Skills include:

- Define and analyze types of criminal behavior in the context of cyber security: fraud/theft, terrorism, extortion, assault, and trafficking and identify the depth and breadth of cybersecurity from multiple perspectives
- Identify organizational / cyber security constraints and decision criteria
- Be able to identify different types cyber attacks / schemes: brute force attacks, ransomware, data breaches, illicit traffic, phishing, and denial of service
- Understand basic regulations - both U.S. and global - and be able to articulate some of the fines / punitive consequences
- Identify methodologies and actions for implemneting cyber security
- Evaluate cyber security alternatives
- Choose the best cyber security solution
- Formulate and present cyber security solutions

Communications Skills

The course exercises develop's various aspects of communication and presentation skills including:

- Knowledge and practice in communicating technical details of modern technology threats in a brief and clear manner, including implications and prescribed actions to mitigate these risks
- Knowledge and practice in producing meaningful presentations and graphics including Infographics

- Presentation skills to including presenting to an audience of employers, mentors, academics/educators and attendees during the final presentations.

Strategy Skills

The ultimate goal is to enable the student to get creative and dissect a scenario in identifying the depth and breadth of the challenge, generating excitement and interest defending against cyberspace based threats and threat actors across multiple disciplines. In other words, based on your perspective, you will focus on the interrelated dimensions (technical, procedural, legal, behavioral, skills/proficiencies) and the spectrum of constituent cyber domains and functional areas to identify solutions.

Course Delivery, Format, & Grading

Course Delivery

This course is offered in an online-blended learning format. All of the lecture materials and assignments will be available on the iQ4 Platform. The course schedule will be distributed to students at time of registration. Students work in teams (cohorts) during the course meeting time throughout the term (four weeks).

Each cohort of students will be broken into teams. The teams will complete assignments in-class on a weekly basis, based on one of the case studies outlined within the syllabus which will also include a final presentation.

There are two (2) individual assignments that are submitted to the iQ4 platform.

Every week will have mentor interaction.

The course will progress as follows:

1. Introduction / Cybersecurity One-on-One [Week 1]
2. The NIST Framework Case Studies [Weeks 2 - 3]
3. Final Presentation - [Weeks 4]

Textbooks/The iQ4 Platform

There are no required printed textbooks for this course. Resources assignments will be available on the iQ4 platform, especially given the rapid-moving nature of Cybersecurity, students and teams will need to supplement the provided materials with online research. The iQ4 platform also includes discussion boards where students, instructors and mentors post questions and general discussions regarding Cybersecurity events.

In addition, the iQ4 platform provides each student with a digital passport that is used to provide a digital transcript evidencing successful completion of the course, an inventory of each student's knowledge, skills and abilities, and to help students identify career pathways.

Session Format

Each session will be broken into two discrete parts – The Lesson portion and the Assignment portion.

The Lesson Portion - Typically, each session's start-up will be based on the Lesson material for that week which will lead into to a discussion on the day's team assignment.

The Assignment Portion - In each session, teams are required to deliver a 10-minute presentation using PowerPoint to the mentors based on the Assignment for that day. This presentation will then form the basis for discussion with the mentors and will also contribute to the student grades.

The instructor will be available for student consultation via phone and Zoom video conferencing during announced office hours and by appointment.

Case Study

The following case study, broken down into four (4) areas are provided to give you an understanding of the complexities involved with insider threats. Your team will use this case study throughout the semester.

Grand Fenwick Healthcare

- **Fraud**:
  In late June 2018, Grand Fenwick Healthcare (GFH) identified activity within its computer network indicating that a cyber- attack may have occurred. An initial investigation was launched immediately to determine scope and depth of attack, and to determine whether or not assistance of an independent computer forensics firm or law enforcement was needed. The investigation revealed that the attack was initiated on June 17, 2018. It has been determined that GFH computer systems that process credit card payments in food and beverage outlets at some GFH locations were accessed by unauthorized persons, resulting in the copying of approximately 21,000 credit card numbers.

- **Theft**:
  Further investigation determined that the cyber attacker(s) may also have gained access to a number of GFH servers, containing personal and patient information of approximately 3.7 million individuals, including patients and providers. GFH decides to publicly disclose the events on August 3, 2018, and law enforcement and appropriate regulatory authorities have been notified. Following discovery, GFH implements actions to remove the malware, remedy the damage to the network, and enhance the security of its network.

- **Extortion**:
  On July 15th, a threat actor sent an email (written in Russian) to the GFH CEO demanding payment of 30BTC or they will publically release GFH patient PHI data to the public. Frustrated at the time it is taking for GFH to respond, the threat actors expand their operation. Using a new variant of what appears to be Petya/NotPetya, the threat actors release the malware on the hospital's operational systems - IoT devices, computers aiding surgical procedures, hospital ward systems for patient care. The threat actors raise the price of the ransom to 60BTC. GFH has also directly notified those individuals which it can identify as potentially having had their personal and patient information improperly accessed, and is offering ongoing monitoring and other steps to protect those who may have been affected by the breach.

- **Trafficking**:
  Due to the publicity of the event and the need to get back online, GFH leadership makes the decision to pay the ransom. A third-party vendor is contacted and negotiations are made. The threat actors demand escrow services are utilized which will take approximately 5 days to complete (as of November 5, 1BTC = 6,413USD). Upon payment, the threat actors release the decryption key, though not all systems are able to be decrypted. Because the malware could have introduced new vulnerabilities to the environment, full wipe and restoration is advised. The threat actors did not release the PII to the public, but the third-party vendor did find evidence that the patient records were up for sale in several illicit marketplaces for $5 record.

Project Role Profiles

- **Cyber Security Attorney:** Handles legal matters related to the internet, e-commerce and data privacy and security. Focuses on the storage and management of information within computer networks and cyberspace, and on everything that happens in connection with data transmitted and stored on computers, including consumer protection laws, privacy laws, e-commerce, and e-discovery issues.

- **Security Operations Center Manager:** Responsible for working in a 24x7 Security Operation Center (SOC) environment. Investigate, document, and report on information security issues, risks, and cyber-attacks. Coordinate with Intel analysts on melicious activities impacting organization. Integrate and share information with other analysts and other teams.

- **Law Enforcement with Specialization in Cyber Crime / Digital Forensics:** Gather, analyze, or evaluate information from a variety of sources, such as law enforcement databases, surveillance, intelligence networks or geographic information systems. Use intelligence data to anticipate and prevent organized crime activities, such as cyber-crime, cyber-attacks, and terrorism. Knowledge of digital forensics software / tools to recovery deleted data and provide an audit trail for criminal prosecution. Presents evidence and testifies in court hearings as a subject matter expert.

- **Insurance Investigator Negotiators (Ransomware/Extortion):** Investigate, analyze, and determine the extent of insurance company's liability concerning personal, casualty, or property loss or damages, and attempt to effect settlement with claimants. Correspond with or interview agents, witnesses, or claimants to compile information. Calculate benefit payments and approve payment of claims within a certain monetary limit.

- **Chief Financial Officer:** The chief financial officer position is accountable for the administrative, financial, and risk management operations of the company, to include the development of a financial and operational strategy, metrics tied to that strategy, and the ongoing development and monitoring of control systems designed to preserve company assets and report accurate financial results.

- **Threat Actor:** A threat actor, also called a malicious actor, is an entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact -- an organization's security. In threat intelligence, actors are generally categorized as external, internal or partner. With external threat actors, no trust or privilege previously exists, while with internal or partner actors, some level of trust or privilege has previously existed. The actor may be an individual or an organization; the incident could be intentional or accidental and its purpose malicious or benign.

Course Grading

10% Individual Assignments

30% Platform and Discussion Board Participation

30% Team Assignments

30% Final Presentation

100% Total

Cyber Crime

The Darker Side of the Web

Epic Challenge

Couse Outline

Course Description

The **Epic Challenge** "Cyber Crime: The Darker Side of the Web" is a survey course of the myriad ways in which the connectivity of the modern world can both benefit and threaten our daily lives. This knowledge has been paired with the basic skills and techniques needed to detect, analyze and defend against these cyber threats. Students from a variety of technical and non-technical backgrounds will have an opportunity to learn about the threats associated with various technologies, as well as the skills needed to analyze, remediate and ultimately defeat those threats. In addition to instruction provided by course faculty, the course includes industry experts serving as mentors to bring real-world experience into the classroom. The course uses the iQ4 applied learning platform and provides a survey of various web actors and activities, including major attack vectors presented by state-sponsored, non-state and organized criminal group actors, utilizing case studies to highlight critical skills needed for the modern virtual warrior. Five modules (The Internet of Things, The Dark Web, Encryption, Cryptocurrency, Weaponization of Social Media) address threats. Students work on cases with different job roles (ex. Cyber Attack Team, Cyber Defense Team, Law Enforcement). The content of the course covers student core competencies (knowledge, skills, and abilities) relating to the case scenarios studied. The course also strengthens essential soft skills, such as teamwork, critical thinking, and communications, which are required in the workforce. The assignments in this course are designed to assess both core competencies and soft skills.

Learning Outcomes

Practical Skills

The course format requires that students operate as project teams addressing challenging scenarios within a case study and/or scenarios involving a fictional company addressing an advanced, persistent web-based threat. Students will conduct online research to assist with addressing the challenges posed by the current landscape and rapidly evolving, emerging technologies. Students will also develop their project management skills. The assignments are project team based and will require students to define responsibilities to ensure fair distribution of the workload and will need to plan their weekly activities to meet the deadlines. Specific Skills include:

- Identify organizational / cyber security constraints and decision criteria
- Be able to identify different types of cyber attacks
- Identify methodologies and actions for implemneting cyber security
- Evaluate cyber security alternatives
- Choose the best cyber security solution
- Formulate and present cyber security solutions

Communications Skills

The course exercises develop's various aspects of communication and presentation skills including:

- Knowledge and practice in communicating technical details of modern technology threats in a brief and clear manner, including implications and prescribed actions to mitigate these risks

- Knowledge and practice in producing meaningful presentations and graphics including Infographics
- Presentation skills to including presenting to an audience of employers, mentors, academics/educators and attendees during the final presentations.

Strategy Skills

The ultimate goal is to enable the student to get creative and dissect a scenario in identifying the depth and breadth of the challenge, generating excitement and interest defending against cyberspace based threats and threat actors across multiple disciplines. In other words, based on your perspective, you will focus on the interrelated dimensions (technical, procedural, legal, behavioral, skills/proficiencies) and the spectrum of constituent cyber domains and functional areas to identify solutions.

Course Delivery, Format, & Grading

Course Delivery

This course is offered in an online-blended learning format. All of the lecture materials and assignments will be available on the iQ4 Platform. The course schedule will be distributed to students at time of registration. Students work in teams (cohorts) during the course meeting time throughout the term (four weeks).

Each cohort of students will be broken into teams. The teams will complete assignments in-class on a weekly basis, based on one of the case studies outlined within the syllabus which will also include a final presentation.

There are two (2) individual assignments that are submitted to the iQ4 platform.

Every week will have mentor interaction.

The course will progress as follows:

4. Introduction / Cybersecurity One-on-One [Week 1]
5. The NIST Framework Case Studies [Weeks 2 - 3]
6. Final Presentation [Week 4]

Textbooks/The iQ4 Platform

There are no required printed textbooks for this course. Resources assignments will be available on the iQ4 platform, especially given the rapid-moving nature of Cybersecurity, students and teams will need to supplement the provided

materials with online research. The iQ4 platform also includes discussion boards where students, instructors and mentors post questions and general discussions regarding Cybersecurity events.

In addition, the iQ4 platform provides each student with a digital passport that is used to provide a digital transcript evidencing successful completion of the course, an inventory of each student's knowledge, skills and abilities, and to help students identify career pathways.

Session Format

Each session will be broken into two discrete parts – The Lesson portion and the Assignment portion.

The Lesson Portion - Typically, each session's start-up will be based on the Lesson material for that week which will lead into to a discussion on the day's team assignment.

The Assignment Portion - In each session, teams are required to deliver a 10-minute presentation using PowerPoint to the mentors based on the Assignment for that day. This presentation will then form the basis for discussion with the mentors and will also contribute to the student grades.

The instructor will be available for student consultation via phone and Zoom video conferencing during announced office hours and by appointment.

Modules

The course begins with an introduction to the world of cyberspace, followed by five focused modules:

Module 1: **Weapons of Mass Disruption - The Internet of Things**

The proliferation of network connectivity in an increasingly diverse number of devices, from washing machines to wearable technology, has exponentially increased the ability to infect and leverage unsecured devices to conduct attacks. While many malicious actors on the internet are seeking to profit from the theft or exploitation of data, the capability to disable or destroy a networked system is an increasingly critical and destructive weapon in the arsenal of state and non-state actors alike. In 2010, a malicious computer worm known as Stuxnet was used to disable Iranian nuclear centrifuges by disrupting industrial control systems designed to maintain operations. Today, the threat of state actors disrupting or destroying critical infrastructure through networks is real and ominous.

Module 2: Plumbing the Murky Depths of the Dark Web

While the indexed portion of the internet, known as the 'surface web', has enabled commerce, sharing of information, and personal expression, more than 85% of the information on the internet has not been indexed by search engines, and is therefore unreachable by most internet users. This is known as the 'deep web'. A small subset of the 'deep web' is subdivided further as the 'dark web', accessible only to those utilizing anonymization and encryption, such as The Onion Brower (TOR) provides. While not originally intended for nefarious purposes, the 'dark web' now infamously a wide array of activities that benefit from anonymity, including online market places where illicit goods and services are openly sold. These goods are typically paid for with cryptocurrencies, further obfuscating the parties involved and protecting them from detection by law enforcement.

Module 3: Encryption – Our Personal Privacy vs. the Public Good

Encryption technology is critical to ensuring the confidentiality, integrity, and security of our most critical data, protecting the content and helping prevent unauthorized access. However, the benefits of encryption are agnostic to intent, and malicious actors utilize encryption for many of the same purposes as legitimate users, including encrypting communications within violent extremist organizations (VEOs), protecting illicit content from discovery, and preventing law enforcement from identifying illegal activity on the darkweb. There is an ongoing and heated debate on how to balance ensuring privacy and security through encryption with preventing or punishing the use of this encryption for criminal or destructive purposes.

Module 4: Cryptocurrency – an Epic 21st Century Gold Rush!

Consumers today are faced with a dizzying array of new technologies, from self-driving cars to gloves that double as cell phones. However, some of the most disruptive technologies being developed today likely escape the notice of most. For example, distributed ledger technology (DLT), made somewhat infamous as the rails for cryptocurrencies like Bitcoin (BTC), is being applied across a variety of sectors, from supply chain management to transaction settlement, loan tracking to identity authentication, and much more. Cloud-based analytics of data collected from biosensors measuring moisture, nutrients, weather and more are revolutionizing the way our food is grown. Machine learning and artificial intelligence are being leveraged in bioengineering to modify the genetic code of plants, animals and potentially people, while nanobots may be a solution to the catastrophic loss of honey bees, the world's chief pollinators.

Module 5: The Weaponization of Social Media and Your Data

In the modern world, it is becoming increasingly common for people to be connected to the global network 24 hours a day. Social media, for example, consumes more of the average person's time than any other activity except sleep and work, and many would rather do without their partner than their mobile device. All of our activities on these devices produce data – clicks, visits, purchases, 'likes', views, and so on. This data is being aggregated and analyzed to create a remarkably detailed profile of our person, our conscious and subconscious preferences, our social circles, and even our health. Social media platforms, for example, have mined the treasure trove of our seemingly innocuous activities

for advertising revenue, as well as social research. Malicious actors have used this information to influence personal choice. But our digital footprint includes much more – the geolocation data mined as we walk around with our device in our pocket, our heartrate and health data mined as we wear our fitness watches, sleep data derived from the movement of our phones, and so on. For many businesses today, the challenge is not how to obtain enough data about you, but how to exploit the incredible amount of data already being collected. For you, the challenge is how to protect yourself, how to control access to data you don't wish to share, and how to identify when your digital doppelganger is being used as a weapon against you.

Project Role Profiles

- Cyber Attack Team - Also known as a red team is a group of white-hat hackers that attack an organization's digital infrastructure as an attacker would in order to test the organization's defenses (often known as penetration testing).

- Targeted Company Cyber Defense Team - Operations that are conducted in the cyber domain in support of mission objectives. Cyber defense focuses on sensing, detecting, orienting, and engaging adversaries in order to assure mission success and to out-manoeuver that adversary.

- Law Enforcement - Members act in an organized manner to enforce the law by discovering, deterring, rehabilitating, or punishing people who violate the rules and norms governing that society.

Course Grading

10% Individual Assignments

30% Platform and Discussion Board Participation

30% Team Assignments

30% Final Presentation

100% Total

IT Audit

Epic Challenge

Couse Outline

Course Description

In this **Epic Challenge**, students from a variety of technical and non-technical backgrounds will have an opportunity to learn about information technology audit, the standards, best practices and what an audit program is, as well as some of the skills needed to conduct a risk assessment and execute an IT audit. In addition to instruction provided by course faculty and assistants, the course involves industry experts serving as mentors to bring real-world experience into the classroom.

Students will become "IT Audit Interns" and work in teams with a faculty member and industry experts as mentors using the iQ4 online/cloud communication platform. The goal is to enable students to analyze IT audit cases in Network Security Audit, Cyber Security Audit, Web Application Security, and Compliance and identify the depth and breadth of IT audit from multiple perspectives. The content of the case studies, covers student core competencies e.g., knowledge, skills, and abilities relating to IT audits including how to build and maintain communications with executives, peers and regulators. Assignments are designed to assess both core competencies and essential (soft/professional) skills.

Learning Outcomes

Upon completion of the course, students should be able to acquire the following:

***P**ractical Skills* - Contextual awareness and knowledge of information technology audit best practices and frameworks, procedures, methodologies, and audit programs.

Communication Skills - Knowledge and practice in producing executive briefing material/memos, Infographics, succinct slide deck presentations and videos on the projects/case studies worked-on. In addition, 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 “IT Audit” challenge), and a crash course in networking prior to the final presentation.

Strategy Skills - 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.

Course Delivery, Format, & Grading

Course Delivery

This course is offered in an online-blended learning format. All of the lecture materials and assignments will be available on the iQ4 Platform. The course schedule will be distributed to students at time of registration. Additionally, students need to allocate time for online team meetings throughout the term (four weeks) of the course.

Each cohort of students will be broken into teams. The teams will complete assignments on a weekly basis, based on one of case studies outlined within the syllabus which will also include a final presentation. Each assignment must be uploaded to the iQ4 platform by the due date.

The course will progress as follows:

7. Intro / IT Audit One-on-One [Week 1]
8. The COBIT Framework Case Studies [Weeks 2 - 3]
9. Final Presentation – Case Study [Week 4]

Textbooks/The IQ4 Platform

There are no required printed textbooks for this course. Resources assignments will be available online on the IQ4 platform but, especially given the fast-moving nature of information technology audit, students and teams will need to supplement the provided materials with online research. The iQ4 platform also includes discussion boards where students, instructors and mentors post questions and general discussions related to information technology audit.

The IQ4 platform is also used by student and teams to post their weekly deliverables and by instructors and mentors to review/assess and provide feedback on the deliverables.

Lastly, the IQ4 platform also provides each student with a digital passport that is used to provide a digital transcript evidencing successful completion of the course.

Session Format

Each session will be broken into two Discrete Parts – The Assignment Portion, and the Lesson Portion.

The Assignment Portion - In each session, teams are required to deliver a 5-minute presentation using PowerPoint to the mentors based on the Assignment for that week (slides must be uploaded by due date with any/all supporting documents). This presentation will then form the basis for discussion with the mentors and will also contribute to the student grades.

The Lesson Portion - Typically, each session's concluding portion will be based on the Lesson material for that week which will lead into to a discussion on the following week's assignment.

The instructor will be available for student consultation via phone and Zoom video conferencing during announced office hours and by appointment.

- ***Required Readings:*** There are no required printed textbooks for this course. However, there are several required readings which will be available through the iQ4 platform.
- ***Attendance and Contribution Policy:*** Students are required to attend every mentor session, unless they have a documented excuse. Additionally, students are expected to contribute to weekly discussions and threads on the iQ4 platform. Students are required to make at least one significant contribution to a discussion every week.
- ***Assignments:*** All assignments need to be submitted by the day/time they are due. If assignment is not submitted on time, the grade earned will be reduced by 50%.

- ***Style Manuals and Guidelines:*** Written assignments and papers should be word-processed and double-spaced in Microsoft Word. Students are required to cite sources, if any are used in their written reports.

The program will start with an introduction to information technology audit followed by a case study. At the conclusion of the second stage, the students will begin to work on their final presentation.

At intervals throughout the course, students may also be required to create and submit short videos for viewing by the mentors.

Case Study

The following four (4) case studies are provided to give you an understanding of the complexities involved with information technology audits. Your team will use one of the case studies to follow throughout the project.

Case Study 1: Network Security Audit

A mid-size telephone company with many entities was concerned about network security. Management wanted an internal and external network security review (audit) of each entity. The audit should include a risk assessment and review of the following:

- Policies, procedures, and plans
- Service providers
- Security associated with servers, firewalls, and network infrastructure
- Protection against malicious software (viruses and spyware)
- Security mechanisms and practices
- Controls over removable media and USB devices
- Incident response and business continuity

The review should include a comparison of the organization with security best practices to identify gaps.

In addition, a report on findings and recommendations and a prioritized risk response executive summary action plan needs to be prepared. The prioritized action plan should help the telephone company increase security and protect its information assets.

Case Study 2: Cyber Security Audit

A county needed assurance that its sensitive information was protected against hackers and other Internet threats. County management was concerned about compliance related issues and wanted assurance its systems were protected against external threats. An External Network Security Audit was

requested. The audit should include the use of a variety of hacker-type tools and techniques that can identify and evaluate the county's external risks to include looking at:

- Firewalls – review and analyze configurations
- External penetration – evaluate vulnerabilities
- Social engineering – determine employee risks
- Phishing – use of fake e-mails and USB devices
- False web sites – determine risks
- Policies – evaluate security related policies

The deliverables should be an External Network Security Audit Report, a Risk Assessment Report, and a prioritized Action Plan Report of security related recommendations. The prioritized Action Plan should help the organization increase security while increasing protection of its information assets.

Case Study 3: Web Application Security

A software developer provides on-line marketing solutions including web design, content management, and e-commerce solutions. The software developer was notified by a third party that it's software was not secure. When negative publicity appeared in the media, clients and prospects became concerned and revenue declined. The software developer's President wanted assurance that its code, with interfaces to internal database systems, was secure and protected from threats.

Using a variety of manual and automated tools, perform a controlled real-life attack on the organization's web application and web server for vulnerabilities. Evaluate the web application for different types of risks, including SQL injection, cross site scripting, buffer overflow, authentication, encryption, and JavaScript. Provide a Web Application Security Audit Report with findings, an analysis of vulnerabilities, and solutions to enhance security.

The organization's enhanced image and reputation will help it increase revenue both by retaining current customers and by converting new prospects into clients.

Case Study 4: Compliance Audit

A large regional hospital needed assurance that health information was protected against unauthorized access. The hospital needed to meet HIPAA and HITECH compliance requirements. A HIPAA / HITECH Compliance and Security Audit was requested. The hospital's security controls need to be evaluated including:

- Administrative Safeguards - policies, procedures, plans, forms, security training, incident response, business continuity
- Physical Safeguards - controls over access to data centers, cameras, EPHI

- Technical Safeguards - firewalls, server configurations, network segmentation, anti-malware, logging, backups

Reports need to be prepared that document areas that place the organization at risk of compliance and the network related threats. An Action Plan Report also needs to be prepared to provide a prioritized risk response plan for the hospital with ways to enhance security, ensure protection of its information assets, and meet compliance requirements.

Course Grading

30% Individual Assignments (Labs)

20% Individual Participation

20% Team Projects

30% Final Presentation

Total 100%