Proposed Degrees in Applications of Cyber Security

As peoples' lives and careers have become increasingly reliant on computers and the Internet, terms like "cyber attack," "hacktivism," "phishing," and "malware infection" have entered into the national lexicon, many undesirable events also have become a part of everyday life, both personally and professionally. In today's world of pervasive computing, everyone has become a target. The volume, sophistication, and effectiveness of the attacks continue to grow and show no sign of abatement. And yet, the ability to recognize vulnerabilities, detect threats, and avoid falling victim to attacks is a skill that many people still lack. It has become critical for organizations to not only protect their assets from outside threats but its time they integrate cyber security in all aspects of their processes, products, and services.

Traditionally cyber security has been delegated to a set of cyber security professionals that take on both the role of defender and the role of cyber security integration. The primary model used by a majority of organizations to integrate cyber security into their processes, products and is services is one where the cyber security team provides input and, in many cases, plays the sole provider of cyber security expertise. This is due in part to the lack of cyber security knowledge by the domain experts who are in charge of the processes, products, and services. It is often easier for the cyber security experts to just bolt security onto what the domain expert produces.

We in academia have mostly focused on building a cadre of individuals who specialized in security of computer and networks as their job. This focus is evidenced by the increase in the number of Centers for Academic Excellence (CAE) schools since the program started with from 7 in 2000 to over 200 in 2019. We educate highly technical individuals who take courses to specialize in the protection of networks, servers, computers, and data. However, because the cyber battle field surrounds everyone and every day, not just the experts, but security warriors also need to be armed.

We are proposing a new model to help integrate cyber security into an organization where non-specialists need to be contributors in the process. We believe this can be done by teaching the fundamentals for cyber security and then building on that foundation by teaching how to apply cyber security to various domains. The proposed Minor in Applications of Cyber Security and the Graduate certificate in Applications of Cyber Security are designed to fill this educational gap.

Our goal is to develop a minor program and a certificate program that teaches students how to apply cyber security. This project goes beyond the traditional cyber security student and/or the computer science student who has security as the focal point of their job. The Applications of Cyber security degrees will prepare students who will design products or solutions for society and who will also need to consider the security implications of their designs. The goal is not to convert students into cyber security experts but to develop the foundations of security so that these students can influence designs and push for integration of security into products, processes, and everyday life. The main benefit of these programs would be development of a work force that has a deeper understanding of cyber security that will increase the cyber security preparedness of an organization.

Target audience

The two degrees are designed to meet the needs to two different target audiences, as summarized in the table below. The undergrad minor will consist of 15 credits and is targeted at current ISU students in non-computing domains. The undergrad minor will start with a set of foundational cyber courses followed by a set of elective courses designed to dovetail into the student's undergrad degree. This allows the student to double count 6 of the credits with their primary major degree.

The graduate certificate is targeted at the off-campus working adult, but will be available to on-campus students as well. The graduate certificate will use the same foundational courses used in the minor followed by a set of graduate level courses and a required case study (capstone) course. The goal is to design a certificate that can be completed in one year.

It is critical that we map each course and modules to the NIST/NICE framework. This allows companies to assess the (KSA) knowledge, abilities, and skills of the students that have completed the degree.

	Undergrad minor	**Grad Certificate**
Credits	15	12
Students	Currently enrolled ISU students	Working Adults ISU Students
Admission requirement	None	B.S. degree with certain GPA or B.S. degree with 5 years of work experience or Current ISU Grad students
New courses	5 credits – Foundation (common) 4 credits	5 credits – Foundation (common) 7 credits
Existing courses	6 credits	

Structure of the Graduate Certificate

The graduate certificate will consist of 12 credits. The courses used in the certificate will be divided into 3 categories. This allows for the certificate to be customized to the needs of an individual student. The graduate certificate will be designed to be completed in 12 months and will be cohort based.

- Foundational courses (5 credits): These 300/400 level courses are common between the undergrad minor and graduate certificate.
- Skills courses (5 credits). These graduate level courses are designed to build off the foundation and develop skills in various areas of cyber security. As the certificate expands there might be more than 5 credits which will give students a choice. We may also identify some skills courses that could be shared with the minor.
- Cyber Security Project course (2 credits): This course is designed to be the culminating experience and will require students to work on a project in context of their discipline.

All of the courses in the graduate certificate will be offered as half semester courses and with the exception of the project course will be one credit each. Two possible example programs of study are provided below:

9 Month completion

Term	First half	Second Half
Fall	3 foundation courses	2 foundation courses 1 skills course
Spring	3 skills courses	1 skills course Project course

12 Month completion time

Term	First half	Second Half
Fall	3 foundation courses	2 foundation courses
Spring	3 skills courses	2 skills courses
Summer	Project course	

If the program grows, as expected, we will on-board new students in each semester.

Structure of the undergrad minor

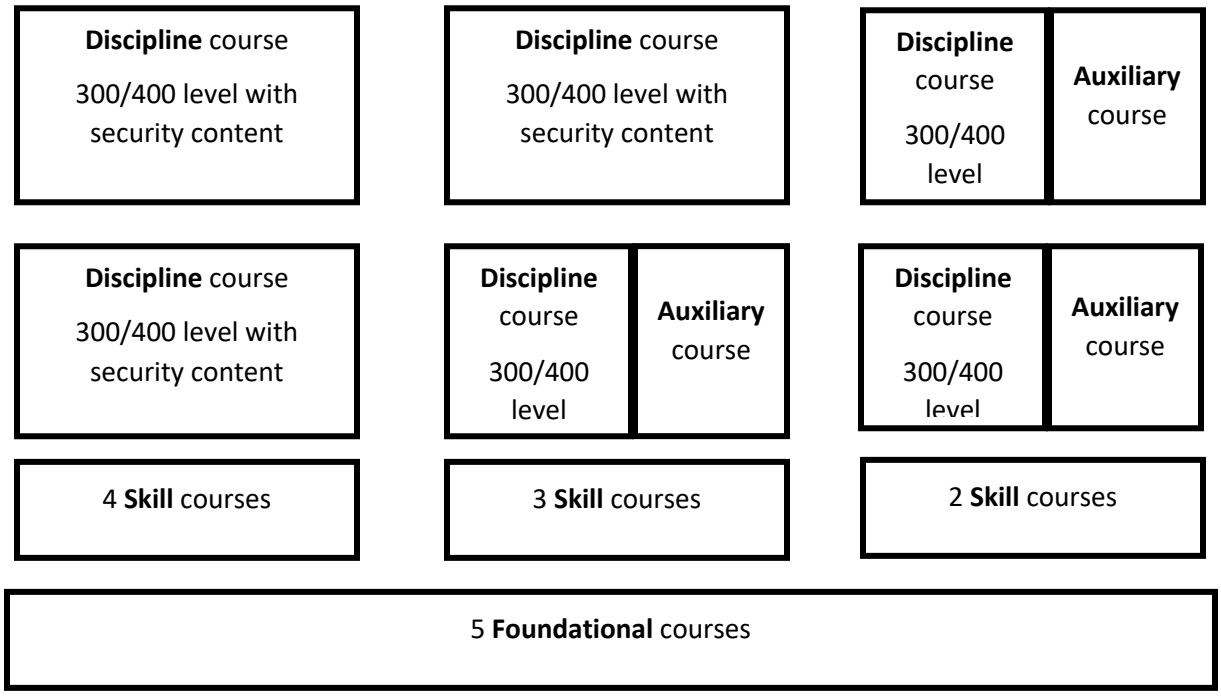
The minor will consist of 15 credits. The courses used in the minor will be divided into 3 categories. This allows for the minor to be customized to the needs of an individual student.

- Foundational courses (5 credits taken by all students)
- Skills / auxiliary courses (4 credits from a list based on the students major / interest). The Skills courses will be designed to work with multiple majors, and the auxiliary courses are designed to support a specific course.
- Discipline courses (6 credits at the 300/400 level in the students major, which are counted in both the student's major and the minor).

We would work with departments across campus to identify the courses that would work as the discipline courses. In some cases, we will design auxiliary courses that would be taken in the same or the following semester as a discipline course which will provide security context to the discipline course. This will provide more focused coursework based on the student's major.

The figure below shows three different scenarios for the minor using different combinations of specialty/auxiliary courses and discipline courses.

1. The first scenario is where all 4 credits of specialty courses are taught independent of the two discipline courses in the major. In this scenario the discipline courses in the major will have some security content.
2. Scenario two one of the courses in the major has security content and the other course the security content is added by the student taking an auxiliary course that the same time as the major course.
3. The third scenario both major courses have an auxiliary course to add the security content.



Structure of the courses / modules

The proposed cyber security foundational and skills courses will be 1 credit each and will be offered asynchronously via Canvas. Each course will consist of a set of modules (between 5 and 10) totaling 15 contact hours. Each course will follow the same format as shown below: An example course is outlined at the end of this document.

- Course introduction / checks for understanding and misconceptions
- Multiple modules
- Posttest / assessment

The structure of a module is shown below:

Delivered content				Post content activities	
Video	Assessment/ Activity/ Checks for understanding	Video	Assessment/ Activity/ Checks for understanding	Lab / Research	Reflection paper

The videos will be 5 to 20 minutes long and will have post video assessment and/or activities. The post video assessment will be designed to be auto-graded with feedback. After each module there will be assigned work which could consist of a lab component, additional research, and/or a reflection paper. The post module assessment may require an instructor / TA to evaluate.

Student / Faculty interaction

To facilitate student to student and student to TA interaction we will use discussion boards. These will be used for general discussions of topics within a course.

Each course will start with “checks for understanding” and “identification of misconceptions.” This will be used by the TA to populate a discussion thread to address the misconceptions and to help fill any gaps that where identified.

Each essay / reflection paper will be read by the TA and feedback will be provided.

The TA will also interact with the students via Canvas messaging to answer specific questions. We could also hold virtual office hours via some type of chat room.

Proposed foundational courses and modules:

Each course / module will be mapped into the NIST/NICE framework

Introduction to cyber security

- What is cyber security
- Computing concepts
- How the Internet works
- The adversary
- Ethics

Digital identity and Authentication

- What is a digital identity
- HIPAA, Laws, Privacy, Personally Identifiably Information (PII)
- What is authentication
- Authentication threats
- Authentication mitigation

Cyber security and the web

- How does the world wide web work
- Attacks against the web
- Common mitigations

Email & malware

- How does email work
- Attacks using email
- Malware / viruses

Social threats

- Social Engineering
- Social Media, Fake News

Possible Skill courses:

- Wireless
- IoT
- Risk assessment
- Supply chain
- Cryptography / cryptocurrency
- Cyber security tools
- Pen testing
- Threat intelligence
- Special topics

Relationship between the applications of cyber security minor/certificate, the cyber security minor and the cyber security engineering degree.

With the introduction of the applications of cyber security minor ISU will have four pathways for undergraduate students. The B.S. degree in cyber security engineering is a technical degree designed for students interested in a career in cyber security. The minor in cyber security is also technical and is intended for students in MIS, Computer Engineering, Computer Science, and Software Engineering. These are student that wish to add a cyber security focus to their primary degree. The minor / certificate in applications of cyber security is designed for students in a non-computing discipline and will allow them to gain knowledge about cyber security in context of their discipline.

Example Course:

Below is a table showing an example course on digital identity and authentication.

Module	Topic	In module Assessment	Homework
1 1 hour	Introduction: a series of videos showing how authentication is used and showing the bad things that can happen.	We would start with a short assessment to determine any misconceptions and what level of knowledge	Short essay: Write a short CNN style news report about something bad that could happen if authentication failed.
2 2 hours	Digital identity and Authentication:	Checks for understanding	Short essay
3 6 hours	Passwords: • Uses • Threats • PW strength • PW secrecy • Web authentication	Checks for understanding	• Password lab on Hackerville. • Short essay / reflection • Research technologies
4 1 hour	Internet of things	Checks for understanding	Short essay
5 1 hour	Mobile Devices	Checks for understanding	Short essay
6 2 hours	Multi factor authentication	Checks for understanding	Password lab on Hackerville.
7 1 hour	Wrap up	Post course assessment	Final reflection paper