Journal of
Information
Systems
Education

Volume 35
Issue 4
Fall 2024

# *Teaching Tip*
# Leveraging Scrum to Increase Student Engagement and Skill Building in Information Security Management

Leigh A. Mutchler, Amy J. Connolly, and Daniel E. Rush

**Recommended Citation:** Mutchler, L. A., Connolly, A. J., & Rush, D. E. (2024). Teaching Tip: Leveraging Scrum to Increase Student Engagement and Skill Building in Information Security Management. *Journal of Information Systems Education*, 35(4), 422-437. https://doi.org/10.62273/KAYG2225

**Article Link:** https://jise.org/Volume35/n4/JISE2024v35n4pp422-437.html

| | |
|---|---|
| Received: | December 6, 2023 |
| First Decision: | April 24, 2024 |
| Accepted: | June 12, 2024 |
| Published: | December 15, 2024 |

ISSN: 2574-3872 (Online) 1055-3096 (Print)

*Journal of Information Systems Education, 35(4), 422-437, Fall 2024*
https://doi.org/10.62273/KAYG2225

# *Teaching Tip*
# Leveraging Scrum to Increase Student Engagement and Skill Building in Information Security Management

**Leigh A. Mutchler**
**Amy J. Connolly**
Department of Computer Information Systems & Business Analytics
James Madison University
Harrisonburg, VA 22807, USA
mutchlla@jmu.edu, conno3aj@jmu.edu

**Daniel E. Rush**
Department of Information Technology & Supply Chain Management
Boise State University
Boise, ID 83725, USA
danrush@boisestate.edu

## ABSTRACT

Information systems courses must adapt to meet the unprecedented demand for well-trained information security (InfoSec) professionals, but they cannot competently fill this gap without also ensuring that students are fluent and confident in foundational skills, both technical and behavioral. How to teach behavioral topics in InfoSec management is not as well covered as topics such as how to configure and apply technology-based security tools. This teaching tip describes how we leveraged the flexibility of the Scrum framework to adapt an InfoSec Management course to meet industry demands. We utilized the framework to provide a mechanism for students to tailor material to their interests while still reinforcing core InfoSec Management content. Following the application of this framework, students reported greater confidence in their ability to pursue InfoSec careers, greater understanding of InfoSec, and additionally found the course interesting and enjoyable. This teaching tip will interest anyone teaching InfoSec Management from a top-down approach as well as those looking to adapt introductory courses in InfoSec or other concept-heavy courses to appeal to a broad base of students.

**Keywords:** Information security management, InfoSec, Agile framework, Scrum, Active learning, IS education

## 1. INTRODUCTION

As organizations increasingly pursue a digital transformation strategy, they must also increase their information security (InfoSec) workforce (Stone, 2022; Thinyane et al., 2022). As of 2022, the Cybersecurity Workforce Gap is estimated at 3.4 million people (ISC2, 2022). Shortages in the InfoSec workforce have persisted since before 2010 (McGladrey, 2022; Oltsik, 2011). Practitioners report that graduates of IS programs enter the workforce without the knowledge, skills, and abilities that organizations desperately want (Mickos, 2019); students report a lack of confidence that prevents them from applying to entry-level jobs. Academic institutions are attempting to reduce these disparities in a myriad of ways (Hennick, 2020). We present one such solution to meet this demand by increasing students' confidence, engagement, and interest in InfoSec Management.

InfoSec is a complex sociotechnical system (Zimmermann & Renaud, 2019) responsible for ensuring the confidentiality, integrity, and availability of the data and systems that are vital to the health of most organizations today (Fitzgerald, 2024). Computer science (CS), information technology (IT), and information systems (IS) programs train students in technology basics, thus preparing students to enter the workforce and fill numerous career paths involving technology and its use in organizations. CS and IT programs focus primarily on technology, and IS programs stress the importance of the human component. InfoSec courses often lean towards mastery of technical topics, even within IS programs. Yet it may be more important than ever for InfoSec professionals to understand the behaviors of people. For example, sophisticated security systems that defend against external bad actors can be defeated by an ill-trained good Samaritan. In InfoSec, people are the weakest link; therefore, they must also be included in the solution (Wilson & Hash, 2003; Zimmermann & Renaud, 2019). We posit that the IS field is uniquely poised to train professionals to defend against human behavior, and that an

InfoSec Management curriculum needs to address these issues in a rigorous yet flexible way.

This teaching tip details our experience redesigning and refining an InfoSec Management course. The primary goals for this redesign were to increase student engagement with behavioral InfoSec concepts and their confidence pursuing InfoSec careers. By using the Scrum framework parallel to the structure of the course, we helped students develop both core and individually selected InfoSec skills, teamwork, and lifelong learning habits. Following guidance provided by Lending & Vician (2012), the presentation of the course redesign begins with first identifying the needs that prompted this redesign. We then present a brief literature review that we used to identify core content and learning theories, followed by a detailed description of our course redesign and evidence from students. Finally, we summarize classroom experiences from the instructor's perspective, including lessons learned, limitations, and contributions to pedagogy.

## 2. NEEDS IDENTIFICATION

The InfoSec Management course is taught every fall and spring semester as an elective in a Computer Information Systems (CIS) program at a large public university in the Southeastern United States. Enrollment ranges from 25 to 35 students per semester. In Fall 2018, the original course followed an introductory, lecture-style model. It was designed to cover a broad range of content without diving deeply into any one topic. At that time, the course focused more heavily on technology-related topics such as network protection devices, but devoted little time to describing how humans interact with, misuse and circumvent technologies. InfoSec continues to rapidly grow and expand. As the gap between technology and human behavior grows ever wider, it became increasingly difficult to identify what to include, expand or exclude in the course. With too much detail, students might feel overwhelmed and disengage; but with too little detail and broad coverage, students might lack confidence in their ability to apply the knowledge, discouraging further study. Therefore, the instructor first identified a need to determine a logical balance between the breadth and depth of material.

The instructor also noted that students reported feeling discouraged from applying to InfoSec job vacancies due to listed experience requirements (House, 2021). Students did not see the connection between the course and the job requirements. This led to the instructor identifying a second need to provide students with experiential opportunities where they both learned core InfoSec concepts and also applied that knowledge. These experiences might build students' confidence to apply to entry-level jobs. Thus, as part of the redesign the instructor identified top skills for entry-level InfoSec professionals.

One such important entry-level skill for InfoSec professionals is teamwork (Marquis, 2019; Pratt, 2023). InfoSec professionals often work in teams because teams tend to be more effective than individuals, particularly when work is complex and ambiguous and requires creativity and problem-solving (Marquis, 2019; Pratt, 2023). Teamwork benefits the team members by providing "positive interdependence, individual and group accountability, interpersonal and small group skills, face-to-face promotive interaction, and group processing" (Laal & Laal, 2012, p. 491). In effective teams, members benefit from feelings of camaraderie and social connection. These positive effects contribute to employees' sense of belonging and job satisfaction (Alvi et al., 2020; Tripp et al., 2016), which, for the organization, contributes to retention (Pratt, 2023).

Successful teams require an array of soft skills such as communication, collaboration, time management, adaptability, and emotional intelligence. Research shows that soft skills can be taught through engaging experiential learning (Sancho-Thomas et al., 2009). Therefore, it was important for the course redesign to make the material more engaging and increase students' confidence in their skills. After identifying how the course needed to change, the instructor reviewed the literature to determine the appropriate level of core content for maintaining rigor and to identify a learning framework to guide the redesign.

## 3. LITERATURE REVIEW

### 3.1 How to Identify "Core Content" in InfoSec Management?

Our review of pedagogical research related to InfoSec revealed that it is generally taught within CS, IT, and IS programs. Most InfoSec programs focus on technical concepts rather than socio-behavioral material (Cram & D'Arcy, 2016). The resources available to teach technical InfoSec concepts through hands-on methods are plentiful (Kim et al., 2023; Liu & Mackie, 2006; Salah et al., 2015; Sharma & Sefchek, 2007; Vykopal et al., 2021), unlike active learning resources for behavioral content (Ahmad & Maynard, 2014; Spears, 2018; Yates et al., 2018). No single clear and concise InfoSec "core curriculum" exists yet (Yates et al., 2018); therefore, for this redesign, we identified and reviewed the two most relevant and current curricular guides. First, the Cybersecurity Curricula 2017, produced by the Joint Taskforce on Cybersecurity Education (CSEC2017) (Burley et al., 2017) to support the development of an interdisciplinary cybersecurity academic program, includes a set of knowledge units to represent the full body of knowledge for the cybersecurity field. Next, the IS2020 Competency Model for Undergraduate Programs in Information Systems (IS2020), produced by the Joint ACM/AIS Task Force (Leidig et al., 2021), provides a competency-based model curriculum for the IS field. Security topics are included throughout the set of ten required competencies, including one titled Secure Computing. The set of core concepts selected for this course, shown in Appendix A, are based on the CSEC2017 knowledge units of Data Security, System Security, Organizational Security, Human Security, and Societal Security, along with the competencies in the IS2020 Secure Computing Competency Area reproduced in Figure 1.

### 3.2 Identifying Theories of Learning to Guide the Redesign

Once we identified the core content to include in the course, we looked for learning theories and teaching methods to guide the redesign. For the readers' benefit and to explain our thought process, we briefly review theories and related teaching methods that we considered for this redesign: sociocultural learning, lifelong learning, active and collaborative learning, flipped classrooms, and Scrum. We blended elements from each of these methods, as none were a perfect fit on their own.

InfoSec is a dynamic field, and professionals must stay abreast of current issues and technologies to be successful within the field. A lifelong learning mindset is often recommended, but multiple definitions of lifelong learning exist. Here, we define it as voluntary, self-directed learning for the purpose of professional development (Valamis, 2022). Vygotsky's theory of Sociocultural Learning (SCL) (McLeod, 2018; Wang, 2007) identifies one way to encourage lifelong learning. SCL states that learning is constructed through interactions within a social system, and that there are two learning levels: one individual may reach on their own and a higher level that relies on help from others. Vygotsky labeled the gap between the two levels as the "zone of proximal development" (ZPD) (Eun, 2019; McLeod, 2018; Wang, 2007), and lifelong learning is one example of ZPD *in praxis.* Furthermore, while an individual must be open to and motivated to expand their learning, they rarely accomplish deep learning on their own; they rely on social systems and the influence of others. Thus, to encourage students to adopt lifelong learning habits, we sought a course redesign that encouraged social-based learning.

Competencies: Graduates will be able to:
1. Explain the purpose of cryptography and how it can be used in data communications
2. Describe the concepts of authentication, authorization, access control, and data integrity and how it helps to enhance data security
3. Explain the security requirements that are important during software design
4. Analyze the concepts of identification, authentication, and access authorization in the context of protecting people and devices
5. Analyze the importance of social media privacy and security
6. Illustrate how cyberattacks work, how to avoid them and how to counteract their malicious consequences
7. Describe risk management techniques to identify and prioritize risk factors for information assets and how risk is assessed
8. Illustrate the types of security laws, regulations, and standards within which an organization operates

**Figure 1. Secure Computing Competencies (reproduced from Leidig et al., 2021, p. 116)**

When students are appropriately motivated, an increase in "learning persistence and performance" can result (Kam et al., 2020, p. 1). Therefore, as part of the course redesign, we also needed to identify a way to increase students' motivation to learn. Among the many teaching approaches available, we began with active and collaborative learning because they are commonly recommended for increasing student interest and engagement. Active learning is a broad term for any teaching method wherein students actively do something in class for the purpose of learning rather than passively listening to a lecture (Fink, 2003). Collaborative learning is one example of active learning in a team setting (Laal & Laal, 2012). In collaborative learning, each group member shares responsibility for learning, using differences across member experiences and understanding to more efficiently and deeply construct their own knowledge. Thus, active and collaborative learning methods made sense for this course redesign for multiple reasons.

Finally, a flipped classroom is a student-centered learning model where students actively participate in their own learning (Mok, 2014). Students prepare for class outside of formal meeting time via assigned readings and videos. Class time is then used for active learning exercises such as homework problems, case discussions, and model building (Bridges, 2017). We chose a flipped classroom model because it could be used to combine teamwork with active and collaborative learning models; it also provided additional class time to build students' confidence in applying their InfoSec knowledge. However, these learning models did not provide guidance related to IS teams in particular. For this aspect, we turned to IS pedagogical literature to find a guiding framework.

Scrum is one example of a framework that could provide flexibility and improve teamwork. The literature contains a few examples of Scrum used in IS courses (Adkins & Tu, 2019; Babik, 2022; Baham, 2019; Rush & Connolly, 2020; Sharp et al., 2020) as well as other disciplines including industrial engineering (Dinis-Carvalho et al., 2019), chemistry (Vogelzang et al., 2019), professional writing (Pope-Ruark et al., 2011), and English studies (Jurado-Navas & Munoz-Luna, 2017). Unfortunately, no ready examples of a Scrum framework for an InfoSec course were found, but we recognized that Scrum's principles matched the skills and goals of this course redesign. Therefore, we next identified how to adapt Scrum to meet our needs.

We did not want to add a project in the course nor did we want to emphasize project management concepts in the course. However, we identified two examples in the literature, Cubric (2013) and Rush and Connolly (2020), where Scrum was used to organize a course's learning activities. Cubric (2013) used Scrum to divide learning materials for a master's level project management course into a series of team assignments. Teams created wikis of an "agile-opedia," which was an encyclopedia of agile project management concepts. The product backlog consisted of topics for the agile-opedia, and the wiki project was divided into five Sprints. In Rush and Connolly (2020), the product backlog items were end-of-chapter exercises and simulated "running cases" from the course textbook. Similar to the InfoSec course, students did not complete an iterative-type semester-long project on a single set of requirements. While not InfoSec-specific, this Scrum framework was sufficiently flexible that we could adapt it to the InfoSec course structure.

After reviewing relevant theories of learning and recent IS pedagogical research, we determined that a flipped-classroom approach used in parallel with the Scrum framework would help us achieve our multi-faceted goals. Although it is most associated with software development, the developers of the Scrum framework define it as "a lightweight framework that helps people, teams and organizations generate value through adaptive solutions for complex problems" (Schwaber & Sutherland, 2020, p. 3). The framework is well-suited for our course for at least three reasons: (1) it embraces change and the learning necessary for the highly-dynamic field of InfoSec. The relevance of particular examples or exercises is enhanced if the teaching method can respond to opportunities in the external environment as they occur; (2) it is team-based, and InfoSec responses typically require cross-functional teams. A teaching approach that mimics this environment becomes professionally relevant; and finally, (3) practicing team self-management with guided reflection allows for important soft skills such as teamwork, leadership, and self-motivation to be learned and ingrained. This concept of self-organizing teams was a particularly attractive strength of the Scrum approach. By encouraging student teams to reflect on team processes, to create ground rules, and to independently resolve conflicts, we expected they might learn important, difficult soft skills. This form of teamwork could also enable social and active learning, and as students successfully completed work, they would build confidence in their skills (Bridges, 2017; Fink, 2003; McLeod, 2018).

An additional benefit of Scrum is that we expected the agile framework could allow us to potentially capitalize on mid-semester opportunities to explore contemporary developments in professional practice in-depth without derailing the rest of the semester's material. For instance, on any given day, InfoSec professionals know their priorities can shift because of factors beyond their control. In the classroom setting, a large-scale data breach might happen mid-semester, or a new technology such as ChatGPT could appear, raising relevant questions about how course concepts can be applied to these novel (and unpredictable) developments. By incorporating this widely recognized IT project management approach in the context of information security, we sought to equip students (and the instructor) to navigate calmly through the chaos an InfoSec professional might face on any given day. After identifying the potential fit of Scrum with our needs, we then determined how to apply it to the course design.

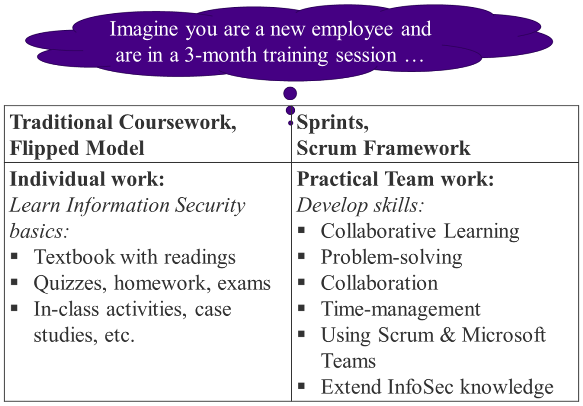
## 4. THE COURSE REDESIGN

Informed by literature, we identified course learning outcomes consistent with the IS2020 (Leidig et al., 2021) and cybersecurity academic programs curricular guide (Burley et al., 2017). These resources also helped us identify core concepts that all students are expected to learn (see Appendix A), and useful topics that students should pursue based on their own interests and career specializations. The flipped classroom model was adopted and combined with the Scrum framework to organize the course. To apply the flipped model, all students are assigned the same individual readings, videos, and quizzes prior to class meetings to support development of "know what" knowledge (Burley et al., 2017; Leidig et al., 2021). We devised a class schedule (see Table 1) in which students actively participated in activities such as case studies, current event discussions, guided research, and other active learning to reinforce concepts. These in-class experiences are designed to engage students with the core content of the course. Alongside the in-class activities, teams collaborate on Sprint work items. We designed the work items either to reinforce a core concept, extend a core concept with greater detail, or provide a self-directed option for students to select material that would expand their knowledge and practice specific skills of interest to them (see Appendix B for examples of each).

We adopted an extended "employee training" metaphor (Figure 2) to create the perception among students that they were participating in a semester-long project. This approached helped students visualize the structure of the course and embrace the use of the Scrum framework. Specifically, we asked students to imagine themselves as new hires working through an InfoSec training program at their new jobs. Their manager (as played by the course instructor) asked them to expand their subject matter expertise on several InfoSec topics relevant to the company and then report back. In Scrum terminology, the manager/course instructor represents the "Product Owner." In effect, this scenario empowers students to envision themselves as InfoSec professionals.

| Outside of Class | In-class Tuesdays | In-class Thursdays |
|---|---|---|
| Course:<br>• Read assigned readings<br>• Create personal notes<br>• Complete terms lists<br>• Answer Review Questions<br>• Take Reading Quiz<br>Scrum:<br>• Sprint Daily Standup | Sprint Planning<br>Course, week activities such as:<br>• Discussions<br>• Review Questions<br>• Case studies<br>• In-class activities<br>• Current news<br>• Guided research<br>• And more … | Course activities such as:<br>• Discussions<br>• Review Questions<br>• Case studies<br>• In-class activities<br>• Current news<br>• Guided research<br>• And more … |
| Course:<br>• Read assigned readings<br>• Create personal notes<br>• Complete terms lists<br>• Answer Review Questions<br>• Take Reading Quiz<br>Scrum:<br>• Sprint Daily Standup<br>• Sprint Deliverable<br>• Sprint Retrospective | Course, week activities such as:<br>• Discussions<br>• Review Questions<br>• Case studies<br>• In-class activities<br>• Current news<br>• Guided research<br>• And more … | Sprint Review<br>Course content conclusion:<br>(time permitting) |

**Table 1. Example Flipped Class Schedule in Parallel With Scrum Framework**



Imagine you are a new employee and are in a 3-month training session …

| **Traditional Coursework, Flipped Model** | **Sprints, Scrum Framework** |
|---|---|
| **Individual work:**<br>*Learn Information Security basics:*<br>▪ Textbook with readings<br>▪ Quizzes, homework, exams<br>▪ In-class activities, case studies, etc. | **Practical Team work:**<br>*Develop skills:*<br>▪ Collaborative Learning<br>▪ Problem-solving<br>▪ Collaboration<br>▪ Time-management<br>▪ Using Scrum & Microsoft Teams<br>▪ Extend InfoSec knowledge |

**Figure 2. Metaphor Explaining Use of Scrum for Coursework**

Students worked in persistent Scrum teams over the full semester. Each team identified specific work items they wanted to complete for each Sprint from a product backlog provided by the Product Owner. Each Sprint included standard Sprint retrospectives, standup meetings, and Sprint reviews to round out the agile team experience. The semester began with a pre-Sprint period, during which students learned about InfoSec terminology and foundational models, the Scrum framework, and Microsoft Teams (MS Teams). The MS Teams platform (Microsoft, 2022) is included in the university-provided Microsoft 365 suite at no cost to students and is secured with dual-factor authentication tied to their student credentials. It encourages student team collaboration by providing real-time communication, file- and app-sharing capabilities, and virtual meeting capabilities. Students quickly adopted it as a team collaboration tool.

Each 16-week semester is divided into four or five 2- to 3-week Sprints with each Sprint including the Sprint Planning, Daily Standup, Sprint Review, and Sprint Retrospective events as illustrated in Figure 3. Students are assigned to teams of four or five, with each team member serving as Scrum Master for at least one Sprint. The team size and makeup depended on course enrollment numbers and what was most convenient for the instructor. We matched the team size to the number of Sprints because it allowed each person to practice as Scrum master. As we gained experience and student feedback, we made some adjustments to team formation such as varying the level and presence of technical and managerial skills levels within teams. Further discussion of enhancements and lessons learned from team formation is provided in Section 7.

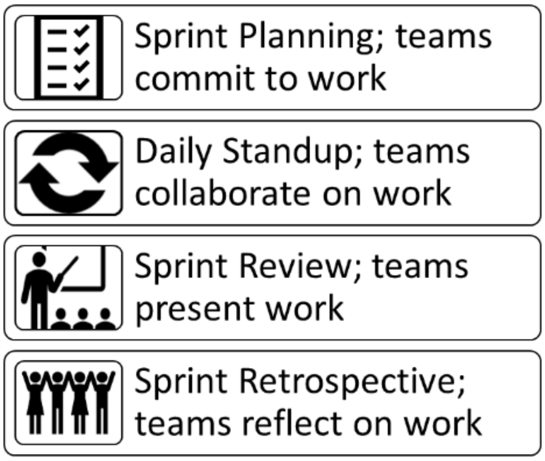

Sprint Planning; teams commit to work
Daily Standup; teams collaborate on work
Sprint Review; teams present work
Sprint Retrospective; teams reflect on work

**Figure 3. Sprint Events**

Each Sprint kicked off with the Sprint Planning event, held in class at the first session of every Sprint. During the Sprint Planning event, teams selected a set of work items from a Sprint product backlog. The backlogs consisted of work items that required students to dig more deeply into core learning items or were self-directed items to allow students to expand beyond the core. These elements of choice allowed students to personalize their learning while ensuring adequate coverage of core concepts. The product backlogs are cumulative, meaning that after the first Sprint, teams could choose previous Sprint work items that they had not previously completed.

Unique to this course redesign, each Sprint's Product Backlog includes the option of a "choose your own" open-ended work item. Teams are strongly encouraged to create their own work items to dive more deeply into a given topic or to highlight material of special interest to them. For example, if a student has work experience such as through an internship, they can leverage that experience. Or if a core topic in the course or a previous Sprint work item particularly interested them, they could explore it more deeply. Such self-directed learning is intended to increase interest and excitement for InfoSec and to build lifelong learner skills (Valamis, 2022) as well as to support development of other capabilities and further encourage students to pursue an InfoSec career. In addition, these choose-your-own activities provide an avenue for the whole class to engage with new topics and perspectives. Each Sprint provides opportunities for students to choose how they applied their knowledge either by developing "know how" skills or expanding their "know what" knowledge.

Student teams are provided 10 to 15 minutes of class time for the Sprint Planning event to discuss the work items in the Product Backlog. During this time, teams ask questions about the work items before deciding which ones to commit to their Sprint backlog. Once they select their work items, teams submit a form listing which items they will complete for the Sprint (the instructor is flexible about teams changing items, but few choose to do so). Teams are expected to complete the work items outside of class time, including the standup sessions and retrospectives.

At the end of each Sprint, teams submit a deliverable consisting of the completed work items formatted as a report (see Appendix C). The Sprint Review is held the next class session. One full class session is dedicated to the Review to ensure that no team is rushed, allowing plenty of time for questions and proximal learning through discussion. Each team presents a unique work item to the rest of the class with a formal presentation. After the presentation, teams submit their presentation materials which include an annotated set of slides and any other presentation materials used during the Review. The presentation materials are also shared with the entire class as a contribution to the collaborative learning and engagement of the course. After the Sprint Review, teams submit a report of their Retrospective to reflect on what they learned as a team and how they plan to improve their work processes in the next Sprint. This course structure has been used for each semester since Fall 2020, with minor modifications and refinements each semester based on student feedback and performance.

## 5. EVIDENCE OF STUDENT ENGAGEMENT AND SATISFACTION

The course redesign presented in this teaching tip is a method of teaching developed primarily to help students better engage with InfoSec Management concepts. Our goals for this model were to improve student engagement and confidence with the course content, ultimately to encourage them to pursue InfoSec careers. We chose a descriptive approach for this study because the human element of teaching and learning ensures that it will be messy, dynamic, and complex, not structured such as rocket science (Regehr, 2010). To assess the redesigned course's success, we examined primarily the rich qualitative evidence, sourced from the free text student responses captured in the in-class activities, Sprint deliverable reflections, mid-semester surveys, and the university's end of course evaluations. Each semester we added a varying set of survey items to the university's end of course evaluations to gain additional student insights. From the Spring 2023 through the Spring 2024 semesters, we collected responses to a consistent subset of items. This subset provided us with quantitative student responses to further support the qualitative responses.

In line with our descriptive approach, we performed a thematic analysis of the free text responses. We identified the four themes of engagement and satisfaction, students' confidence in pursuing InfoSec positions, Scrum and teamwork, and self-directed learning. Student feedback examples representative of each theme are presented next along with descriptive statistics of the supporting quantitative responses where appropriate.

### 5.1 Engagement and Satisfaction

Students report feeling engaged and satisfied with the course. They consistently indicated that they liked the course design and content. Each semester we received comments such as "I love the course I wouldn't change anything about it," [it was] "fun, enjoyable, and beneficial learning experience. Loved the class format …," "I loved this course because it was extremely practical and will be my most influential class post-graduation," "This was my favorite class this semester and though it covered a lot of material, it felt very manageable and the class structure made me enjoy learning the content," "It was good, interesting course structure that I think will benefit me in the long run," and "it is an interesting class, you learn a lot and it covers a wide breadth of infosec subjects without getting too deep in to any one subject." When students are more interested and engaged with topics, they learn more and become lifelong learners (Connolly et al., 2022; Eder et al., 2019), which are invaluable goals for InfoSec professionals.

One of the survey items included in course evaluation surveys provided further evidence of student engagement and satisfaction with the course design. The item captured student perceptions about the use of collaborative learning in the course. The chart in Figure 4 shows that out of 55 student responses, 43 (78.2%) agreed that collaborative learning improved their learning experience.

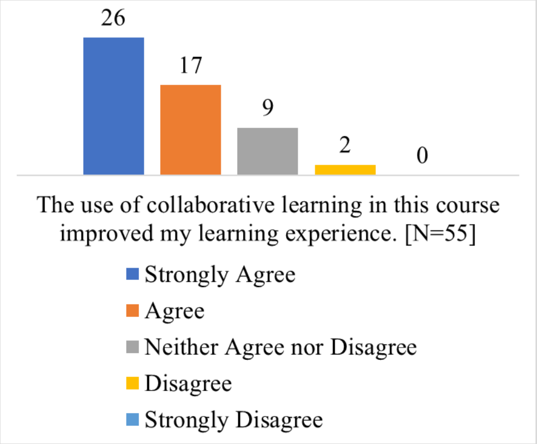


**Figure 4. Student Appreciation of Collaborative Learning**

### 5.2 Confidence in Pursuing InfoSec Positions

Students report a greater understanding of and appreciation for the behavioral side of InfoSec, which is one of the main goals of this course redesign. "I think that the individual and team work really helped with getting a good understanding of InfoSec," "I think this was a great class that sets the foundation of an InfoSec career path, as a lot of topics were talked about. Just having this fundamental knowledge allows me to explore more concepts surrounding InfoSec," "I think learning the importance of the management side to infosec was very beneficial. I specifically think learning about the identification, authentication, authorization, and accountability concepts will be beneficial in my career," and "I didn't realize how many different components there are to company security. I learned about the different positions and different careers I could pursue."

Figure 5 shows that most students (46 out of 55, 83.6%) agreed their interest in an InfoSec career after taking the course increased, and 43 out of 54 students (79.6%) indicated that they are seriously pursuing a career in the field. This evidence further supports the notion that the course influenced students' confidence to pursue InfoSec positions.

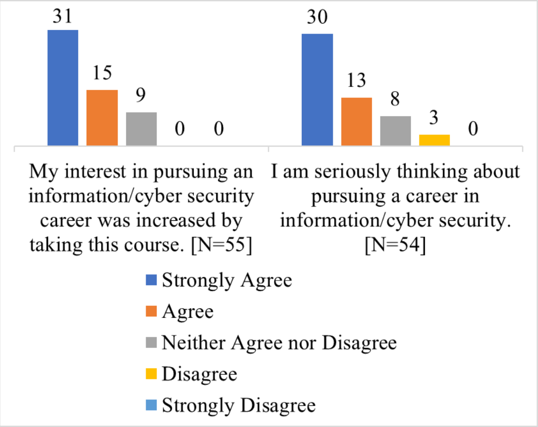


**Figure 5. Effect of Course on Student Career Interest**

### 5.3 Scrum and Teamwork

The comments from students indicate an appreciation for the Scrum framework and associated teamwork. They recognize that both will be useful in their future careers, stating: "I liked working in groups and how long we had to work on each Sprint. I also enjoyed the topics we could choose from," "I thought the class was great, I enjoyed how the Sprints and presentations worked and the time given to get it done," "I loved this class! It gave me a good idea of how Sprints work," "I really liked using SCRUM and Teams to collaborate, it should all stay the same," "[I liked the] opportunity to dive deep into various InfoSec topics. With regards to Microsoft Teams, I think it was a great platform for collaboration between team members. For future class, incorporating both the Scrum framework and Microsoft Teams will allow students to gather a foundational understanding of InfoSec," and "I like the scrum framework in this class. It was something I liked to talk about during my job interviews and my interviewers were interested in learning about what I did. I recommend you keep it up!" These comments are clear indicators that students noticed the effectiveness and feel the course should continue using the redesign.

The surveys conducted during the Spring 2023 to Spring 2024 semesters also included items to assess student perceptions about the course's impact on soft skills. Three of the survey items with responses are shown in Table 2. Most students agreed that the course was beneficial to the development of their collaboration and lifelong learning soft skills, and 36% agreed their time management soft skills improved as well. Figure 6 shows that students perceive the skills practiced in the course as beneficial to their future careers.

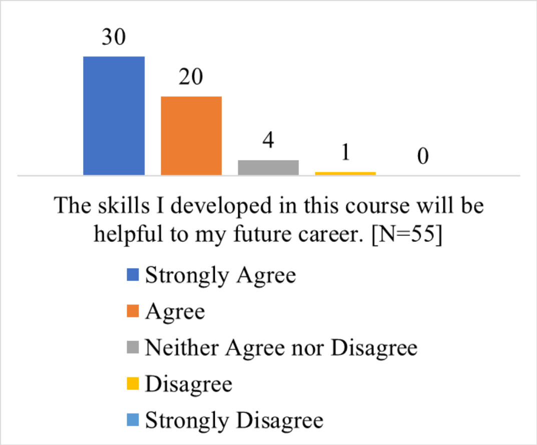


**Figure 6. Student Perceptions of Course Skills**

### 5.4 Self-Directed Learning

Students appreciated the freedom to choose work items that interested them. This was clear from comments such as "I liked the exploration of security related topics that the sprints allowed students to experience," "[I liked the] independent research opportunities," "Letting us pick what we work on was really nice and there was a good range of topics to pick from," "I really liked how the Scrum framework allowed every team member to explore what interests them. By being able to focus on areas of interest, students had the opportunity to dive deep into various InfoSec topics...," and "Overall I thought this course was very beneficial for me as I am hopefully entering the workforce soon and I feel like I have learned great resources to conduct research on to better prepare myself." These comments further support the idea that the course increased students' confidence in their skills and their feeling of preparedness for future InfoSec jobs.

Based on the student feedback evidence presented, we consider this course redesign to be successful at increasing students' engagement, interest, and confidence in InfoSec Management. Next, we discuss evidence from the instructor's experience implementing the redesign over multiple semesters.

## 6. INSTRUCTOR'S IMPLEMENTATION EXPERIENCES

This course redesign includes multiple benefits for the instructor as well, most of which are related to the inherent flexibility of the model. The instructor can react more quickly to changing circumstances such as current events in InfoSec, more easily refine content as those developments occur, and respond to student needs and interests—all without disrupting the flow of the course or confusing students. The instructor typically makes minimal changes to core materials and individual assignments during the semester. Students willingly accept changes to team assignments (often looking forward to them), or to the implementation flow of the course, because of the use of agile within the structure. This combination of static and dynamic, flexible assignments and course flow makes the overall course more engaging and fun.

The team assignments also provide a vehicle for the instructor to safety-test new assignments. For example, after reading a news article about an important and timely InfoSec issue, the instructor could assign the article to all teams add it to the upcoming Product Backlog, allowing the teams to determine the deliverable requirements in collaboration with the instructor. Together, the student teams and the instructor can design an engaging, interesting assignment that the instructor can later adapt for use in future semesters. This approach also encourages students to become lifelong learners.

By focusing the Sprint Review presentations on students' personal takeaways rather than on what work they did, those presentations became more valuable for the entire class, even for teams who completed the same work item. These presentations were also opportunities for students to showcase creativity and pride in their work, which is always a pleasure to witness for an educator. Finally, as students became more deeply engaged in their work, they learned to interpret material in a novel way, teaching the instructor something new and interesting. All told, the instructor gained nearly as much from the course redesign as the students.

| Survey Items [N=55] | SA* | A* | NA* | D* | SD* |
|---|---|---|---|---|---|
| This course provided me with opportunities to improve my collaboration skills. | 36 (65%) | 15 (27%) | 4 (7%) | 0 (0%) | 0 (0%) |
| This course provided me with opportunities to improve my lifelong learning skills. | 29 (53%) | 19 (35%) | 7 (13%) | 0 (0%) | 0 (0%) |
| This course provided me with opportunities to improve my time management skills. | 20 (36%) | 23 (42%) | 10 (18%) | 2 (4%) | 0 (0%) |
| *SA=Strongly Agree; A=Agree; NA=Neither Agree nor Disagree; D=Disagree; SD=Strongly Disagree | | | | | |

**Table 2. Effect of Course on Student Perceptions of Soft Skill Development**

## 7. LESSONS LEARNED AND COURSE ADAPTATIONS

The first major lesson learned, which was key to the direction of the course design, was discovered during the initial implementation of this newly redesigned course. It was the Fall 2020 semester, which also coincided with our institution's first fully online semester during the COVID-19 pandemic. Students were given significant freedoms regarding how they spent class time; due in part to the many uncertainties of the world at that time. Students appreciated the freedoms, stating "… you have made our lives as students much more enjoyable. I'm also extremely grateful for you not hosting class and instead allowing us to meet as a group during class time …" However, it quickly became apparent that a more structured class session was necessary. Since then, the course has evolved through adaptations into its current state—a hybrid mix of a traditional class elements and Scrum components. To support the flipped model, class time is now used for activities such as case studies, current event discussions, guided topic inquiries, and hands-on experiences such as developing a security awareness poster or performing a simple risk cost-benefit analysis. These activities include individual components along with team discussions and reflections to support the collaborative learning goals of the course and to bolster teamwork skills.

When asked to report on what they learned by completing assignments, most students simply provide details about the steps they took to get the job done, stopping short of considering what they got out of the experience. This important lesson learned became most evident during the Sprint Reviews. Teams present the highlights of completed work items, but because the same work items may have been completed by multiple teams, no two teams are allowed to present on the same one. In addition to reducing monotony, this ensures that each team contributes uniquely to the collaborative *learning* of the class by presenting their own "takeaway" from the experience—what they "learned" by completing the work. By sharing those takeaways, the team Sprint Reviews provided valuable contributions to the learning of the entire class. The instructor simply had to gently but frequently remind students to reflect on what was interesting or surprising about the work—the major takeaway that made it worth doing.

Some students did not accept the way Scrum was implemented in this course redesign, and we share some of these lessons learned to help instructors adopting this model in their own courses to avoid similar pitfalls. In the earliest semesters, students with previous Scrum experience pushed back with comments such as "I don't think what we did was scrum, I think we would need to dedicate part of class to creating user stories, stand up meetings, and retrospectives—that's not to say that what we did should change, just that what we did isn't exactly scrum" and "If you intend to keep scrum as a major part of the class, I would recommend creating projects that force greater collaboration between group members—something like creating a system security plan could be a useful exercise and could easily leverage scrum." We expect that as more students practice Scrum in other classes, particularly if they have used it in a more traditional way in project and software-development courses, this resistance (or confusion) may persist. To address this issue, at the start of the course during the pre-Sprint period the instructor emphasizes how the application of Scrum in this course is a valid and valuable way to support cohesive team development and collaboration. Then, reminders are periodically given to students throughout the semester. A flexible mindset is critical to using an agile framework. Students should be encouraged to expand their thinking and embrace an agile mindset in order to fully benefit from collaborative learning.

Some negative student comments about Scrum stemmed from soft skills issues. For example, one student wrote "The scrum project didn't really follow what scrum is except for the backlog and review and allowed for my team members to procrastinate too much and often the work wasn't compiled till the day of the presentation." Another student wrote "when one group member decides to slack off, the entire group suffers." These students blamed Scrum, not realizing that they were actually identifying a poor time management issue. Based on this feedback, we moved the due date of the major deliverable to *before* the Sprint Reviews, to encourage students to better manage their time. We also revised the Sprint Deliverable instructions (see Appendix C), and we put more time into class discussions about time management.

A few students wrote that "the assignments we did in the sprints were very tedious and felt like busy work," and "The whole SCRUM thing adds very little value to the course. The sprints and presentations feel very disjointed." To address these student concerns, each semester, the instructor carefully and mindfully curates the product backlog work items to provide activities that students will find meaningful, interesting, efficient, and effective. Work items that "flop" are removed and new ones added to stay current and keep the material fresh and interesting. These incremental changes have reduced negative comments over time.

The instructor has also varied the number of students on each team from five to four. The Scrum Guide advises to keep teams small, with no more than ten members (Schwaber & Sutherland, 2020). When the course content was easily grouped into five parts, we included five Sprints. We created teams of five so that team members could take turns serving as the Scrum Master role in each Sprint. Over time, course updates impacted the course schedule in such a way that it made more sense to reduce the number of Sprints to four. By reducing the number of Sprints, we increased flexibility and allotted more time for in-class activities. We reduced the size of teams to four to match the number of Sprints.

In terms of how we formed teams, we chose not to allow students to choose their own teams. In compliance with the Scrum Guide's recommendation for cross-functionality on teams, we tried to vary technical and managerial skills and skill levels within teams, which also encouraged collaborative learning (Sancho-Thomas et al., 2009). A more complete discussion about team formation methods is beyond the scope of this paper, but we direct the interested reader to a few suggested resources for further reading (Duke, 2024; Verma, 2020).

As with most courses, we cannot please everyone, but overall, student complaints in this course tend to be typical of those received in most courses. The instructor has used the student feedback along with personal observations to make adaptations each semester to improve the course. For the most part, the changes made have been minor. For example, after receiving comments like "[I dislike] having to do both the readings and the sprint work," "I did not like the focus on the management side" or "[lack of technology] I wanted to learn more hands on Cyber Security stuff," the instructor now includes an extended discussion at the start of the course to better manage student expectations regarding what the course does and does not include.

Although the course redesign met the expected goals, it is not a panacea for typical student complaints. Each semester someone felt the course was too hard or too easy, they disliked the textbook because it was hard to read, was boring, or had poor e-text capabilities, and they found the exams too challenging and wanted them done away with entirely. Finding the right balance among course components is always a challenge. For example, we still struggle with figuring out how much time to spend on in-class activities versus discussion and how much time to give teams during class, if any. Through trial and error, our design has evolved into a course that consists of two parts: a "regular" course and a Scrum extension. The Scrum framework in parallel to the core course adds flexibility, and we believe it can be easily adapted by other instructors for other courses.

The first two iterations of this course redesign were somewhat successful in an online course, and based on the lessons learned since then, we believe the current design would not require much modification to apply in a synchronous online modality. For example, this design would synchronize nicely with an online course that is already structured in a flipped modality. One thing we learned the hard way, however, is not to give teams too much unstructured time during class. Whether in person or online, some student teams will simply opt-out of using this time, therefore wasting precious contact hours. Lastly, we are currently identifying ways to expand this course redesign to larger, in-person classes up to 45 students, such as creating Scrum "teams of teams" (Doshi, 2015), which will require expanding work items to activities that can best be completed by multiple teams working together. We recognize that one limitation of this course redesign is that it may not scale well to classes with more than 50 students.

## 8. CONCLUSIONS AND CONTRIBUTIONS

The existing literature offers minimal general guidance for instructors wanting to design an applied course that focuses on behavioral concepts in InfoSec, and we found no other examples of a course redesign that uses an adaptable agile framework. To address these gaps, we designed and iterated on an InfoSec Management course by using a Scrum framework as a way to extend the course content. This method enabled students to hone their skills while increasing their interest in the material and recognizing the relevance of the course to their careers. This teaching tip presented an innovative method of teaching the behavioral side of InfoSec in an InfoSec Management course. This redesign provided students with the foundations of the field while at the same time giving them the freedom to direct and expand their learning. This approach increased student interest in and engagement with the behavioral side of InfoSec. Students worked in agile teams to build InfoSec Management artifacts, allowing them to self-direct a portion of their learning and to build and practice team collaboration skills. Students reported an increased knowledge of and confidence in their InfoSec abilities and a stronger interest in applying to InfoSec careers post-graduation.

The overall positive nature of student feedback indicated students believe the course format is useful. It helped them to recognize the importance of InfoSec and Scrum skills in their future careers. As a result, students completing the course developed a broader understanding of the types of careers available in the InfoSec field, and they felt better prepared to fill the ever-increasing excess of job openings in InfoSec. As an added bonus, students gained experience using widely-adopted Scrum tools and practiced their soft skills, such as time management, communications skills, and leadership.

One limitation of this paper is the relatively small enrollments in the course, which prevented us from collecting quantitative data from students that might be analyzed beyond merely descriptive statistics. We also did not collect data before the course redesign. To address these limitations, we provided copious feedback from students, lessons learned from the instructor, and suggestions for avoiding potential pitfalls encountered during this redesign, such as student pushback, and how to improve on and maintain this approach after adoption.

This paper's contribution to pedagogical research is particularly relevant due to the extreme need for InfoSec practitioners. We used state-of-the-art tools to support project teams as they solved relevant, real-world InfoSec problems. Through agile, collaborative learning, student teams improved their communication and collaboration skills. Our pedagogical contributions are applicable to face-to-face as well as online course implementations. This redesign will interest instructors and researchers in information security because it provides an easily adopted course design for teaching behavioral concepts and topics in an InfoSec course, and because of the novel application of Scrum. Furthermore, this design could easily be adapted to any concept-heavy introductory course to increase its appeal to a broad base of students.

## 9. REFERENCES

Adkins, J. K., & Tu, C. (2019). Applying an Agile Approach in an Information Systems Capstone Course. *Information Systems Education Journal*, 17(3), 41-49.

Ahmad, A., & Maynard, S. (2014). Teaching Information Security Management: Reflections and Experiences. *Information Management & Computer Security*, 22(5), 513-536. https://doi.org/10.1108/IMCS-08-2013-0058

Alvi, A., Kayani, D. U. S., & Mir, D. G. M. (2020). Relationship of Employee Training, Employee Empowerment, Team Work With Job Satisfaction. *Journal of Arts & Social Sciences*, 7(2), 185-198. https://doi.org/10.46662/jass-vol7-iss2-2020(185-198)

Babik, D. (2022). Teaching Tip: Scrum Boot Camp: Introducing Students to Agile System Development. *Journal of Information Systems Education*, 33(3), 195-208.

Baham, C. (2019). Implementing Scrum Wholesale in the Classroom. *Journal of Information Systems Education*, 30(3), 141-159.

Bridges, F. (2017, July 21). 10 Ways to Build Confidence. *Forbes*. https://www.forbes.com/sites/francesbridges/2017/07/21/10-ways-to-build-confidence/

Burley, D., Bishop, M., Buck, S., Ekstrom, J., Futcher, L., Gibson, D., Hawthorne, E. K., Kaza, S., Levy, Y., Mattord, H. J., & Parrish, A. (2017). *Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity: Vol. Cybersecurity Curricula 2017*. Association for Computing Machinery. https://doi.org/10.1145/3184594

CCECC.ACM. (2023). *Bloom's Revised Taxonomy*. ACM Committee for Computing Education in Community College. http://ccecc.acm.org/assessment/blooms

Ciampa, M. (2018). *CompTIA Security+ Guide to Network Security Fundamentals* (6th ed.). Boston, MA, USA: Cengage.

Connolly, A. J., Mutchler, L. A., & Rush, D. E. (2022). Teaching Tip: Socio-Cultural Learning to Increase Student Engagement in Introduction to MIS. *Journal of Information Systems Education*, 33(2), 113-126.

Cram, W. A., & D'Arcy, J. (2016). Teaching Information Security in Business Schools: Current Practices and a Proposed Direction for the Future. *Communications of the Association for Information Systems*, 39, 32-51. https://doi.org/10.17705/1CAIS.03903

Cubric, M. (2013). An Agile Method for Teaching Agile in Business Schools. *The International Journal of Management Education*, 11(3), 119-131. https://doi.org/10.1016/j.ijme.2013.10.001

Dinis-Carvalho, J., Ferreira, A., Barbosa, C., Lopes, C., Macedo, H., & Tereso, P. (2019). Effectiveness of Scrum in Project Based Learning: Students View. In J. Machado, F. Soares, & G. Veiga (Eds.), *Innovation, Engineering and Entrepreneurship* (pp. 1118-1124). Springer International Publishing. https://doi.org/10.1007/978-3-319-91334-6_154

Doshi, H. (2015, April 15). *A Scaled Scrum Tactic "Team of Teams"* | *Scrum.org*. https://www.scrum.org/resources/blog/scaled-scrum-tactic-team-teams

Duke. (2024). *Making Student Teams Work in Your Course—Duke Learning Innovation*. Duke Learning Innovation & Lifetime Education. https://learninginnovation.duke.edu/resources/art-and-science-of-teaching/using-student-teams-effectively-course/

Eder, L. B., Antonucci, Y. L., & Monk, E. F. (2019). Developing a Framework to Understand Student Engagement, Team Dynamics, and Learning Outcomes Using ERPsim. *Journal of Information Systems Education*, 30(2), 127-140.

Eun, B. (2019). The Zone of Proximal Development as an Overarching Concept: A Framework for Synthesizing Vygotsky's Theories. *Educational Philosophy and Theory*, 51(1), 18-30. https://doi.org/10.1080/00131857.2017.1421941

Fink, L. D. (2003). *A Self-Directed Guide to Designing Courses for Significant Learning*. https://www.deefinkandassociates.com/GuidetoCourseDesignAug05.pdf

Fitzgerald, A. (2024, October 9). *Cybersecurity Explained: What It Is & 13 Reasons Cybersecurity Is Important*. Secureframe. https://secureframe.com/blog/why-is-cybersecurity-important

Hennick, C. (2020, September 30). Training the Next Generation of Cyber Professionals. *EdTech: Focus on Higher Education*. https://edtechmagazine.com/higher/article/2020/09/training-next-generation-cyber-professionals

House, N. (2021, August 8). Is the Cyber Security Skills Gap a Myth? *StationX Cyber Security Blog*. https://www.stationx.net/is-the-cyber-security-skills-gap-a-myth/

ISC2. (2022). *ISC2 2022 Cybersecurity Workforce Study*. ISC2. https://www.isc2.org:443/Research/Workforce-Study

Jurado-Navas, A., & Munoz-Luna, R. (2017). Scrum Methodology in Higher Education: Innovation in Teaching, Learning and Assessment. *International Journal of Higher Education*, 6(6), 1-18. https://doi.org/10.5430/ijhe.v6n6p1

Kam, H.-J., Menard, P., Ormond, D., & Crossler, R. E. (2020). Cultivating Cybersecurity Learning: An Integration of Self-Determination and Flow. *Computers & Security*, 96, 101875. https://doi.org/10.1016/j.cose.2020.101875

Kim, J. B. (Joo Baek), Zhong, C., & Liu, H. (2023). Teaching Tip: What You Need to Know About Gamification Process of Cybersecurity Hands-on Lab Exercises: Lessons and Challenges. *Journal of Information Systems Education*, 34(4), 387-405.

Laal, M., & Laal, M. (2012). Collaborative Learning: What Is It? *Procedia - Social and Behavioral Sciences*, 31, 491-495. https://doi.org/10.1016/j.sbspro.2011.12.092

Leidig, P. M., Salmela, H., Anderson, G., Babb, J. S., Gardner, L., Nunamaker Jr, J. F., Scholtz, B., Shankararaman, V., Sooriamurthi, R., & Thouin, M. (2021). *IS2020 Competency Model for Undergraduate Degree Programs in Information Systems*. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/is2020.pdf

Lending, D., & Vician, C. (2012). Writing IS Teaching Tips: Guidelines for JISE Submission. *Journal of Information Systems Education*, 23(1), 11-18.

Liu, C., & Mackie, B. G. (2006). Teaching Tip: Teaching Security Techniques in an E-commerce Course. *Journal of Information Systems Education*, 17(1), 5-10.

Marquis, A. (2019, February 4). Importance of Teamwork in Organizations. *Small Business - Chron.Com*. https://smallbusiness.chron.com/importance-teamwork-organizations-14209.html

McGladrey, K. (2022, October 17). 4 Stakeholders Critical to Addressing the Cybersecurity Workforce Gap. *Dark Reading*. https://www.darkreading.com/careers-and-people/4-stakeholders-critical-to-addressing-the-cybersecurity-workforce-gap

McLeod, S. A. (2018, August 5). *Lev Vygotsky's Sociocultural Theory*. Simply Psychology. https://www.simplypsychology.org/vygotsky.html

Mickos, M. (2019, June 19). The Cybersecurity Skills Gap Won't Be Solved in a Classroom. *Forbes*. https://www.forbes.com/sites/martenmickos/2019/06/19/the-cybersecurity-skills-gap-wont-be-solved-in-a-classroom/

Microsoft. (2022). *Online and Virtual Meeting Software* | *Microsoft Teams*. Microsoft Teams Online Meetings. https://www.microsoft.com/en-us/microsoft-teams/online-meetings

Mok, H. N. (2014). Teaching Tip: The Flipped Classroom. *Journal of Information Systems Education*, 25(1), 7-12.

Oltsik, J. (2011, January 3). Will There Be a Shortage of Cyber Security Professionals in 2011? *CSO Online*. https://www.csoonline.com/article/2228141/will-there-be-a-shortage-of-cyber-security-professionals-in-2011-.html

Pope-Ruark, R., Eichel, M., Talbott, S., & Thornton, K. (2011). Let's Scrum: How Scrum Methodology Encourages

Students to View Themselves as Collaborators. *Teaching and Learning Together in Higher Education*, 1(3), 17.

Pratt, M. K. (2023, June 12). The 12 Biggest Issues IT Faces Today. *CIO*. https://www.cio.com/article/228199/the-12-biggest-issues-it-faces-today.html

Regehr, G. (2010). It's NOT Rocket Science: Rethinking Our Metaphors for Research in Health Professions Education. *Medical Education*, 44(1), 31-39. https://doi.org/10.1111/j.1365-2923.2009.03418.x

Rush, D. E., & Connolly, A. J. (2020). An Agile Framework for Teaching With Scrum in the IT Project Management Classroom. *Journal of Information Systems Education*, 31(3), 196-207.

Salah, K., Hammoud, M., & Zeadally, S. (2015). Teaching Cybersecurity Using the Cloud. *IEEE Transactions on Learning Technologies*, 8(4), 383-392. https://doi.org/10.1109/TLT.2015.2424692

Sancho-Thomas, P., Fuentes-Fernández, R., & Fernández-Manjón, B. (2009). Learning Teamwork Skills in University Programming Courses. *Computers & Education*, 53(2), 517-531. https://doi.org/10.1016/j.compedu.2009.03.010

Schwaber, K., & Sutherland, J. (2020). *The Scrum Guide. The Definitive Guide to Scrum: The Rules of the Game*. https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-US.pdf#zoom=100

Sharma, S. K., & Sefchek, J. (2007). Teaching Information Systems Security Courses: A Hands-on Approach. *Computers & Security*, 26(4), 290-299. https://doi.org/10.1016/j.cose.2006.11.005

Sharp, J. H., Mitchell, A., & Lang, G. (2020). Agile Teaching and Learning in Information Systems Education: An Analysis and Categorization of Literature. *Journal of Information Systems Education*, 31(4), 269-281.

Spears, J. (2018). Gaining Real-world Experience in Information Security: A Roadmap for a Service-Learning Course. *Journal of Information Systems Education*, 29(4), 183-202.

Stone, M. (2022, January 13). Digital Transformation: Balancing Speed, Security and Innovation. *Security Intelligence*. https://securityintelligence.com/articles/digital-transformation-balancing-speed-security-innovation-cybersecurity/

Thinyane, M., Christine, D., & Detros, K. (2022, October 21). *Beyond Supply and Demand: Addressing the Multidimensional Workforce Gaps in Cybersecurity*. World Economic Forum. https://www.weforum.org/agenda/2022/10/cybersecurity-workforce-gaps-inclusive-approach-jobs/

Tripp, J., Riemenschneider, C., & Thatcher, J. (2016). Job Satisfaction in Agile Development Teams: Agile Development as Work Redesign. *Journal of the Association for Information Systems*, 17(4), 267-307. https://doi.org/10.17705/1jais.00426

Valamis. (2022, February 17). *What Is Lifelong Learning? Its Importance, Benefits & Examples*. Valamis Knowledge Hub. https://www.valamis.com/hub/lifelong-learning

Verma, M. (2020, July 22). Cybersecurity Lessons From the Pandemic. *Dark Reading*. https://www.darkreading.com/vulnerabilities---threats/cybersecurity-lessons-from-the-pandemic/a/d-id/1338368

Vogelzang, J., Admiraal, W. F., & van Driel, J. H. (2019). Scrum Methodology as an Effective Scaffold to Promote Students' Learning and Motivation in Context-based Secondary Chemistry Education. *Eurasia Journal of Mathematics, Science and Technology Education*, 15(12), em1783. https://doi.org/10.29333/ejmste/109941

Vykopal, J., Čeleda, P., Seda, P., Švábenský, V., & Tovarňák, D. (2021). Scalable Learning Environments for Teaching Cybersecurity Hands-on. *2021 IEEE Frontiers in Education Conference (FIE)* (pp. 1-9). https://doi.org/10.1109/FIE49875.2021.9637180

Wang, L. (2007). Sociocultural Learning Theories and Information Literacy Teaching Activities in Higher Education. *Reference & User Services Quarterly*, 47(2), 149-158. https://doi.org/10.5860/rusq.47n2.149

Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security* (7th ed.). Boston, MA, USA: Cengage.

Wilson, M., & Hash, J. (2003). *Building an Information Technology Security Awareness and Training Program* (NIST Special Publication SP.800-50). https://doi.org/10.6028/NIST.SP.800-50

Yates, D. J., Frydenberg, M., Waguespack, L. J., McDermott, I., O'Connell, J., Chen, F., & Babb, J. S. (2018). Dotting I's and Crossing T's: Integrating Breadth and Depth in an Undergraduate Cybersecurity Course. *2018 Proceedings of the EDSIG Conference*, 21.

Zimmermann, V., & Renaud, K. (2019). Moving From a 'Human-as-Problem" to a 'Human-as-Solution" Cybersecurity Mindset. *International Journal of Human-Computer Studies*, 131, 169-187. https://doi.org/10.1016/j.ijhcs.2019.05.005

## AUTHOR BIOGRAPHIES

**Leigh A. Mutchler** is an associate professor of computer information systems and business analytics in the College of Business at James Madison University. She earned her Ph.D. in Management Information Systems from Mississippi State University. Her research interests are primarily in the areas of information security end user behaviors and awareness instruction. She has published her research in the *Communications of the Association for Information Systems*, the *Journal of Information Systems Education*, the *Journal of Computer Information Systems*, *Information and Computer Security*, and the *Journal of Database Management*.

**Amy J. Connolly** is an associate professor of computer information systems and business analytics in the College of Business at James Madison University. Her doctorate is in Management Information Systems from the University of South Florida. Her research interests include the role of social media in volunteer organizations and active learning and inclusion in information systems pedagogy. She has published her research in the *European Journal of Information Systems*, *Communications of the Association for Information Systems*, and the *Journal of Information Systems Education*.

**Daniel E. Rush** is an associate professor of information technology management at Boise State University's College of Business and Economics. He earned his Ph.D. in Business Administration from the University of Michigan. Prior to joining academia, he worked with IT projects in the health care, real estate, telecommunications, and high-tech industries. Dr. Rush researches applying information systems to challenging interdisciplinary problems such as environmental sustainability, as well as topics related to project management and information systems education. His research has been published in the *Journal of Cleaner Production*, *Information & Management*, *Communications of the Association for Information Systems*, and *Journal of Information Systems Education*.

## APPENDICES

### Appendix A. Core Concepts and Skills

The set of core concepts for this course were selected based primarily on the CSEC2017 knowledge units of Data Security, System Security, Organizational Security, Human Security, and Societal Security (Burley et al., 2017), supported by the Secure Computing Competency Area in IS2020 (Leidig et al., 2021) which added a layer of IS specificity:

- Policies and laws
- Ethics and privacy
- Risk management
- Contingency planning
- Identity and access management
- Vulnerability assessment
- Security education, training, and awareness
- Behavioral controls
- Cryptography basics
- Physical security controls

As recommended by CSEC2017, the set of six "crosscutting concepts" listed below in Table A-1 are also reinforced throughout the course.

**Table A-1. Six Crosscutting Concepts (Source: Burley et al., 2017)**

| **Concept** | **Description** |
|---|---|
| Confidentiality | Rules that limit access to system data and information to authorized persons |
| Integrity | Assurance that the data and information are accurate and trustworthy |
| Availability | The data, information, and system are accessible |
| Risk | Potential for gain or loss |
| Adversarial Thinking | A thinking process that considers the potential actions of the opposing force working against the desired result |
| Systems Thinking | A thinking process that considers the interplay between social and technical constraints to enable assured operations |

Both CSEC2017 and IS2020 prescribe skill levels based on Bloom's Taxonomy (CCECC.ACM, 2023), the majority of which are levels 2 (understanding), 3 (applying), or 4 (analyzing). Bloom's levels 1 and 2 are what IS2020 describe as "know what," and Bloom's levels 3 and above as "know how."

The remainder of the core concepts for this course are skills related to the use of teamwork, the Scrum framework, and MS Teams:

- Collaboration
- Decision-making/problem-solving
- Collaborative learning

**Appendix B. Example Sprint Product Backlog**

(Work items were inspired by or are modified exercises from the textbooks by Whitman and Mattord (2022) and Ciampa (2018))

| Description | Points | Type* |
|---|---|---|
| **Choose Your Own Work Item**<br>Learn more about a topic of your choice, prepare training on a topic you already know, or perform some other work of your choice to contribute to the collaborative learning goals of this course. Suggestion: create a learning activity to share your information security-related knowledge gained from internship or job experiences. Provide a short proposal (sentence or two, written or verbal) to the Product Owner to explain the work you wish to do and justify the value of the work (5 vs. 10 points). Approval by the Product Owner may be granted *before or during* the Sprint Planning meeting. | Varies 5-10 | SD |
| **Mafiaboy, Mitnick, and Abagnale**<br>Research the following three individuals: Mafiaboy, Kevin Mitnick, and Frank Abagnale. Write a summary explaining who they are, what they did, and where they are today: Include details about how each is related to the information security field. | 10 | SD |
| **Current Attack Examples**<br>Choose 3 of the 12 threat categories shown in Table 2-5 on p. 34 of the textbook (i.e., Whitman & Mattord, 2022). Perform a Web search to find a current news article illustrating each threat category you chose. Summarize each news article and explain how it represents an example of the category. | 10 | C |
| **NIST Cybersecurity Framework**<br>At the NIST Web site - https://www.nist.gov/, from the Topics menu, select Cybersecurity. On the right side of that page is a Featured Content list – click on Cybersecurity Framework (CSF). Explore the content. What is the CSF and what is it designed for (what is its purpose)? What are the five functions of the framework? (list and briefly explain each). From a big picture perspective, explain how a company could use the CSF. Identify and list two specific areas of the framework that could provide guidance, and explain the type of guidance each could provide. | 10 | C |
| **InfoSec C-Suite Roles**<br>Perform research using the Web to learn more about the security roles of Chief Information Officer (CIO), Chief Information Security Officer (CISO), and “Virtual CISO.” Create a table to compare the roles. Summarize your findings. | 5 | SD |
| **CAPEC**<br>Visit the Common Attack Pattern Enumeration and Classification (CAPEC™) Web site at http://capec.mitre.org. Explore the site to learn about CAPEC and answer the questions: What is CAPEC, why is it important, what problems does it aim to solve, and who benefits from it? | 5 | R |
| **OWASP Top 10**<br>Visit the OWASP Top 10 site at https://owasp.org/www-project-top-ten/#. Who would likely find the content at this Web site useful and why? Find the current Top 10 list at the Web site and compare it to the list found in our textbook (pp. 67-68). How has the list changed, and why do you think that happened? Choose three of the risks from the current list of 10, and explore the content provided about each at the site. Summarize your findings. | 5 | R |
| **Counterintelligence & Security**<br>Explore the National Counterintelligence and Security Center at https://www.dni.gov/index.php/ncsc-home. What type of resources are available at this site? Choose two resources that are of interest to you and briefly describe them, explaining why you chose them. Do you believe this site would be a useful resource for *all* security professionals? Why or why not? | 5 | R |
| **Insider Threat**<br>Search the web for at least three resources that discuss the concept of *insider threat*. Based on the resources found, develop an in-depth definition of the concept. To illustrate it, develop three simple example scenarios of threats that are categorized as insider threats. | 5 | CE |
| **Defense in Depth**<br>Search the web and find at least three resources that describe the concept of defense in depth. Summarize your findings, briefly comparing the three resources. Find the definition of defense in depth in our textbook. What are the similarities and differences? | 5 | C |
| **Network Security Toolkit (NST)**<br>Using the Internet, find at least three Web sites that refer to network security toolkit (NST). Write a brief summary that explains what it is, what it is used for, what its capabilities are, and who might use it. | 5 | SD |
| **NIST**<br>Explore the NIST Web site at https://www.nist.gov/. What does the NIST acronym stand for and what is its purpose? Notice the various resources and topics at the site. Identify and list three topics that look interesting to you and you would like to learn more about. What types of organizations would find the NIST resources useful? List at least three resources that would be useful to our course. | 5 | R |

| | | |
|---|---|---|
| **NIST Special Publications**<br>At the NIST Web site, https://www.nist.gov/, from the Services & Resources menu select the Computer Security Resource Center (CSRC) page. Expand the Publications menu on the left side of the page, and link to view the NIST Special Publications (SPs). Select the SP 800 Series. Scroll through the list, skimming the publications and making a mental note of the topics. Find SP 800-100 and download a copy for review. What is the title of that publication? Briefly describe its contents. Provide your opinion about how this publication could be a good resource for our course. | 5 | R |
| **CHIPS for America**<br>Perform a web search to learn about the CHIPS for America program. Summarize your findings (what, where, when, why, etc.). Explain why (or why not) this program is of importance to our course. | 5 | SD |

* Students were not provided with the Type column. It is included here to illustrate whether the backlog item is an InfoSec resource (R), reinforces a core concept (C), an extension of the core (CE), and/or is a Self-Directed (SD) item meant to be selected based on a student's intrinsic interest.

## Appendix C. Deliverable for Each Sprint

**Instructions:**
The Sprint Deliverable is the reporting of the work completed for the Sprint. Each team will follow these instructions to create the report, and each member will then review the report for completeness and adequacy prior to submitting it for course credit.

1. Create the report using Word
2. Name the file as: TeamName_Sprint#
3. Use professional and consistent formatting, and be sure to include page numbers
4. The cover page includes Sprint#, Team Name, ScrumMaster, and Team Member(s) names
5. Add a table of contents page next with page numbers (using Word formatting can "automate" this for you)

The details of the work done for the Sprint backlog work items are next.

6. Start a new page for each work item, and order the pages in the same order as on the Commitment form. Include the following for each work item:
   a. Work Item Name (as shown on backlog)
   b. Team Members assigned
   c. Brief description of the core problem/work item
   d. Brief statement of why you chose the work item
   **e. An explicit statement about what you learned, i.e., what the major takeaways were from completing the work item**
   f. A potential exam question (multiple-choice, fill-in-the-blank, multiple-answer, or short-answer) with a correct answer
   g. References for this work item.
      i. Use APA style for all resources
      ii. If you used an AI tool, include the Name of publisher/tool producer (year), Name of AI tool (version date), and include a full transcript of the writing or work produced by the AI tool in an appendix to the deliverable

And last:

   **h. The work item results. Depending on the work item, the format used may vary (text, graphic, etc.).**
      i. All work must be your own. The integrity of the deliverable file will be checked with the Turnitin tool in Canvas, so do not just copy/paste from any source used, including from the output produced by an AI tool (if you choose to use one). If you have any questions about the appropriate use of AI, please ask

INFORMATION SYSTEMS & COMPUTING ACADEMIC PROFESSIONALS

## STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the ***Journal of Information Systems Education*** have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN: 2574-3872 (Online) 1055-3096 (Print)