STI Strategic Plan for 2013 - 2017

2013 Strategic Plan Goal 1: Enhance Academic Quality

Achieve and sustain academic quality commensurate with a globally respected graduate school dedicated to enterprise information security leadership.

The goal of enhancing academic quality supports STI's vision of preeminence. STI will continuously assess and improve its world-class technical education programs to ensure that scholarship and research builds student leadership and implementation capabilities and improves the information security systems of their employers. Detailed sub-goals and associated benchmarks are listed below.

1.1. Enhance curriculum offerings for information security leadership by implementing new and more focused curriculum. [Benchmarks: (1) Complete the implementation of MSISM and MSISE Curricula 3.0 by the end of 2015; (2) Conduct ongoing assessments of learning outcomes for updating curriculum; and (3) Complete a comprehensive review of Curricula 3.0 by the end of 2017.]

1.2. Enhance institutional effectiveness by evaluating and implementing a formal faculty recruitment, development, and retention program. [Benchmark: Complete evaluation of potential faculty recruitment, development and, retention program by the end of 2014 and implement the plan in 2015.]

1.3. Support student success by strengthening our enrollment management processes and engaging employers (or sponsors) in a student's choice of electives and research projects. [Benchmarks: (1) Reach graduation rates of 80% within five years; and (2) Increase the proportion of students engaged in employer-supplied research projects to 15% by the end of 2014, and 25% by the end of 2015.]

1.4. Validate the impact and value of an STI master's degree by measuring the satisfaction of STI alumni and their employers, while creating a formal feedback mechanism to improve the curricula. [Benchmarks: (1) Implement a formal alumni tracking and communications program by the end of 2014; (2) Put in place one-year and three-year post-graduation satisfaction measurement systems for both alumni and their employers by the end of 2014; and (3) Use the results of those satisfaction surveys to drive improvements in the curriculum from 2014 through 2017.]

1.5. Select and convene an Advisory Committee comprised of alumni, employers, leading information technology and information security executives and influential thought leaders and scholar-practitioners. This committee will help improve and formalize STI's relationship with employers and the information security community, and improve our ability to assess changing market conditions and inform curriculum improvements. [Benchmark: First Advisory Committee meeting in June, 2014]

2013 Strategic Plan Goal 2: Increase Student Enrollment to Ensure Institutional Effectiveness and Viability

Enable STI to have the scale, staffing, and institutional effectiveness to attain and maintain economic self-sufficiency.

STI's mission and vision require support from a self-sustaining stream of resources. STI needs to have more students completing more credit hours for three reasons: first, to improve the speed with which we create the leaders desperately required by organizations subject to cyber attack; second, to help the Institute itself in its goal to become economically self-sustaining; and third, because achieving and increasing scale will allow us to re-invest in new potential educational opportunities. Goal 2 must be achieved without any sacrifice in quality, and the careful balance of growth, investment, and process management must be consistently assessed and maintained. Detailed subgoals and associated benchmarks are listed below.

2.1. Implement marketing and employer partnership programs to increase enrollment to 250 by the end of 2015 and to 450 by the end of 2017. [Benchmark: Total active enrollment 250 degree-seeking students by December 2015.]

2.2. Reduce the time required for students to complete their degrees. [Benchmark: By 2017, 50% of students complete the STI program within 36 months of the time they enter the program.]

2.3. Increase the realized tuition per credit hour, and completed credit hour per student, to reach economic break-even point at an enrollment of 175 students. [Benchmark: Economic break-even in 2014.]

2.4. Grow and support STI staff and faculty in order to provide world-class academic programs and student services to the increased number of students, as described in the STI Financial and Staffing Plan 2013-2017. [Benchmarks: (1) Develop surveys to determine satisfaction of staff and students by the end of 2013; (2) Measure staff and student satisfaction via annual surveys beginning at the end of 2013; and (3) Maintain satisfaction levels above 90% throughout 2014-2017.]

2.5. Expand the use of the Institutional Effectiveness Plan and integrate it into the ongoing operation of all STI divisions in order to synchronize unit goals, individual staff goals, and institutional goals. [Benchmark: Unit goals reflect institutional goals by 2014.]

2013 Strategic Plan Goal 3: Enhance Quality and Quantity of Research

Maintain an information security research portfolio that establishes STI as one of the nation's most prolific and cutting-edge research centers in information security.

A cornerstone of STI's success is collaborative research. The information security field is constantly evolving and facing new threats; only a research-based curriculum led by scholar-practitioners can hope to maintain curriculum sufficiently up to date to be relevant. STI faculty must be actively engaged in state-of-the-art research and practice (scholar-practitioners) in order to be credible instructors of information security. At the same time, enabling students to participate in active, visible research programs that are developing widely-adopted solutions helps build the students' portfolios and confidence. STI research initiatives enable the faculty to stay current and keep courses up to date, and they afford students opportunities that will enhance their learning experiences and careers, and ultimately contribute to the organization with which they are affiliated. Detailed subgoals and associated benchmarks are listed below.

3.1. Support the development of STI students as scholar-practitioners by expanding the number of students whose research projects are part of, or complement, STI's expanding research portfolio. That portfolio currently includes the (1) Internet Storm Center (cyber threat monitoring and response), (2) Critical Security Controls (consensus prioritized best practices to mitigate enterprise information security threats), and (3) NetWars, CyberCity, and related cyber simulator research. [Benchmark: 35% of STI students engaged in advancing STI-supported research programs by 2015.]

3.2. Create a new research center focused on advancing the state of the art of digital forensics and incident response. [Benchmark: Operational by 2015, nationally recognized and widely used by 2017.]

3.3. Increase the number of research papers by STI faculty, students, and research fellows that are accepted for publication in peer-reviewed journals and for presentation at peer-reviewed professional conferences. [Benchmark: Increase the number of peer-reviewed papers to 20 per year by 2015.

3.4. Expand the use/adoption of the recommendations of STI research programs to improve information security across the United States by developing and implementing outreach initiatives specific to STI's major research programs. [Benchmarks: (1) Increase adoption of the Critical Security Controls to 10% of federal departments and state governments and at least 50 of the Fortune 500 banks, utilities, and industrial companies by 2015; (2) Expand the active use of the Internet Storm Center to more than 15,000 users each day by 2016 and (3) Expand the use of NetWars and CyberCity simulators to more than 2,000 cyber-warrior trainees annually by 2015.]

3.5. Establish a research fellows program and recruit the top information security managers and scholar/practitioners to serve as fellows. [Benchmark: Recruit three world-class research fellows by 2014.]

3.6. Raise the visibility of STI and build its brand by increasing the frequency of STI faculty, research fellows, and alumni being quoted in the press and being called upon for expert guidance by government policymakers and industry leaders. [Benchmark: A program is established in 2014 which informs the press of the availability of STI experts, measures the number instances STI experts are quoted and publishes and maintains an annotated directory of articles referencing STI faculty, researchers, and alumni, as well as a directory of their policy guidance engagements.]

3.7. Expand industry partnership programs established in meeting Goal 2.1 in order to implement industry-specific research programs (e.g., in power, healthcare, oil and gas, banking, etc.) in which interested students and others from those industries work on projects, produce papers, and give research presentations directly relevant to effective enterprise information security for that industry. [Benchmark: One industry-specific research partnership program in place in 2014 and three in 2016.]

3.8. Develop and manage a process to ensure that the results of STI's research programs are actively integrated into the STI course curricula. [Benchmark: Develop an active measurement system by 2014 that assesses the degree to which STI research is reflected in those courses.]

2013 Strategic Plan Goal 4: Achieve and Maintain Accreditation

Ensure that STI has the ability to take advantage of best practices in higher education in order to facilitate continuous improvement and ensure that an STI degree is respected by employers and by professionals seeking postgraduate degrees in information security.

Achieving MSCHE accreditation is a central requirement for STI to meet its mission, and in particular its goal of reaching economic self-sufficiency and growing its reputation in higher education and in the information security practitioner community. Furthermore, a continuing process of assessment and improvement is essential to the continuing health of the institution. Detailed subgoals and associated benchmarks are listed below.

4.1. Conduct the Middle States Commission on Higher education (MSCHE) self-study that integrates strategic planning and academic program review; compile the MSCHE Self-Study Report; and host the MSCHE accreditation team in 2013. [Benchmark: Achieve MSCHE accreditation in 2013.]

4.2. Actively engage in institutional and student learning assessments and continue to use the resulting assessments to improve the institution's effectiveness. Document that process and answer other questions in preparation for the Periodic Report required in 2018. [Benchmark: Establish self-assessment team by the date approved by MSCHE.]

Professionals from across the STI community—the board, administration, faculty, alumni, and others—contributed substantially to updating these goals. The goals reflect the consensus on what it will take for STI to accomplish its mission in order to make a substantial impact on information security in the United States and across the world. Accomplishing those goals in the time we have allotted will be extremely challenging, but the entire STI community shares the urgency of our mission and has demonstrated a willingness to do what it takes to meet the challenge.