Journal of Information Systems Education

Volume 33
Issue 3
Summer 2022

SOC It to 'Em: Bringing a Security Operations Center onto a University Campus

Jim Marquardson

Recommended Citation: Marquardson, J. (2022). SOC It to 'Em: Bringing a Security Operations Center onto a University Campus. *Journal of Information Systems Education*, 33(3), 300-305.

Article Link: https://jise.org/Volume33/n3/JISE2022v33n3pp300-305.html

Initial Submission:	19 November 2021
Accepted:	15 December 2021
Published:	15 September 2022

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

Journal of Information Systems Education, 33(3), 300-305, Summer 2022

SOC It to 'Em: Bringing a Security Operations Center onto a University Campus

Jim Marquardson
College of Business
Northern Michigan University
Marquette, MI 49855, USA
jimarqua@nmu.edu

ABSTRACT

Employers want applicants with experience, even for entry-level cybersecurity roles. Universities traditionally help students gain cybersecurity experience by hiring them for on-campus jobs or by matching job seekers to employers for off-campus work. A third option is described in this paper in which universities bring external companies on campus. Recently, our institution partnered with Novacoast to open a security operations center on campus that employed university students as analysts. Novacoast develops NovaSOC—a security information and event management platform that captures and analyzes information gathered from server and client devices. Interns in our campus security operations center used NovaSOC to monitor security events for Novacoast customers who chose to outsource monitoring to Novacoast. While the security operations center has been a success, establishing it required that the institution address technical issues such as network connectivity and organizational changes like requiring background checks for student employees. Students reported that they would choose to work in the security operations center again but were generally underworked. Administrators reported that the security operations center was aligned with the university's mission but felt that few people at the university truly understood the work conducted in the security operations center. Institutions looking to bring external entities on campus for similar partnerships should engage risk management early, ensure that student staffing matches the expected workload, and develop plans for financial sustainability. This paper delves into the details of bringing a security operations center onto our campus and gives actionable advice for institutions seeking to establish similar partnerships.

Keywords: Cybersecurity, Career development, Security operations center, Security information and event management, Internships & co-ops

1. INTRODUCTION

Cybersecurity threats show no signs of abating (Ben Fredj et al., 2020). Assaults on critical infrastructure, businesses, government institutions, and the democratic process are regular evening news features. Unquestionably, the world needs professionals who can secure information systems. The academies are a critical component for helping develop knowledge and skills, but employers are increasingly looking for hands-on work experience in addition to a degree. Hands-on experience in a work environment helps students learn in part by engaging with more experienced professionals (Lave & Wenger, 1991).

Not all students gain work experience in their field by graduation. In one survey of students pursuing information technology (IT) degrees, 39.6% of students did not have any IT-related job experience (Legier & Soares, 2014). Academic institutions help students gain cybersecurity employment in a variety of ways. Technology abounds in modern academic institutions—from dormitory access control systems, learning management systems, computer clusters that support research, industrial control systems, and much more. The university may employ students to build and maintain these information systems. Also, academic institutions frequently have career centers that advertise positions on job boards and organize career fairs. Internships are encouraged by many institutions, with some institutions offering academic credit for internships (Payne et al., 2020). Increasingly, companies offer virtual internships with geographic flexibility (Pittenger, 2021). Some institutions are beginning to encourage and facilitate apprenticeships to build cybersecurity skills (Stoker et al., 2021).

Our institution sought a novel way to help students gain industry experience while pursuing their education. We partnered with Novacoast—creator of the NovaSOC security information and event management (SIEM) platform. We opened a security operations center (SOC) on campus wherein student interns would analyze data for Novacoast clients. In this model, students gained experience and built their resumes without having to leave campus. Student interns were given training and practical experience monitoring real cybersecurity alerts for businesses.

Setting up the SOC on campus required cooperation from several entities. University risk management, information technology, building services, academic departments, and Novacoast had to answer critical questions over several months before the SOC could be launched.

In March 2020, our institution learned of Novacoast's desire to establish a SOC at an academic institution. We expressed interest and immediately started planning a SOC pilot at our university. The SOC concept was developed over the summer 2020. Formal agreements and technical implementation largely occurred in fall 2020. The SOC opened on campus for training in the last week of January 2021, and alert monitoring began in February 2021.

The purpose of this paper is to describe the motivations for bringing a SOC on campus, the process for managing the SOC implementation, the challenges we faced, lessons learned, and what results other institutions might expect when pursuing similar endeavors. Data from students and administrators are presented and actionable guidance is summarized.

2. SECURITY OPERATIONS CENTERS

A SOC "monitors and manages all aspects of enterprise security in real-time from a single, centralized location" (Kelley & Moritz, 2006, p. 28). Because every device on a network is a potential attack vector, organizations should monitor security-related events from laptops, smartphones, printers, security cameras, and any other device connected to the network. The National Institute of Standards and Technology (NIST) mandates continuous monitoring in its cybersecurity framework (National Institute of Standards and Technology, 2018).

As the number of devices connected to modern networks increases, so does the number of security events that administrators must log and analyze. SIEM platforms aggregate log data from devices on the network, normalize the data, and perform data analysis to find threats (Bhatt et al., 2014). SIEM platforms can analyze data based on signatures, heuristics, or deviations from established baselines. Because automated analysis may miss some malicious activity, administrators employ threat hunting to investigate suspicious events manually.

SOC experience would help students build cybersecurity skills. Because a SOC has visibility into all devices on a network, students would be able to observe various attacks and recommend remediation. The experience would prepare students for later roles as engineers, managers, policymakers, and more.

3. BRINGING A SOC TO CAMPUS

In recent years, our institution created partnerships with several cybersecurity companies. These partnerships can be mutually beneficial by serving the self-interests of both parties (Becker & Brown, 2000). Though many industry representatives were willing to meet and advise our institution on matters of curriculum and strategy, few were in a position to create recurring pipelines for internships or full-time work. A gap existed between our education programs and employment. This section describes our institution and how we formed a partnership with Novacoast to help students gain real-world cybersecurity experience that would propel them forward in their careers.

3.1 Institutional Organization

Our university offers education through traditional degree programs, such as a Bachelor of Science in cybersecurity in the College of Business. We also have a continuing education department that offers professional, workforce, and personal training that focuses on building in-demand skills. For example, the continuing education department offers CompTIA Security+ courses. From an organizational perspective, the two branches operate independently, though there is the opportunity to share resources. The effort to bring a SOC on campus was primarily driven by the continuing education department, but degree-seeking students staffed the SOC.

3.2 Ideation

Novacoast is a cybersecurity company seeking rapid growth in both customers and employees. Like many other organizations, Novacoast recognized the gap between industry demand for qualified employees and the number of job-ready applicants. Novacoast approached representatives from our institution to pilot an on-campus SOC. Students trained in the SOC would be prepared for future careers as SOC analysts or move on to other positions. One reason the institution embraced the partnership with Novacoast was the commitment that Novacoast had to student training and helping students earn experience without expecting students to transition to become Novacoast employees after graduation.

3.3 Physical SOC Requirements

The campus SOC needed to fulfill Novacoast's physical security requirements. Sufficient privacy controls had to be in place to ensure that work done in the SOC was not visible from outside. To prevent shoulder surfing-type attacks, the SOC could not be on a building's ground floor. The SOC also needed access controls to limit who could enter. Fortunately, the room on campus used for cybersecurity training and outreach events was well suited to meet the requirements. The room had card access integrated with student identification cards, sat on the second floor of a building, and had frosted windows that prevented passersby from reading information on computer screens.

3.4 Technical Requirements

Our institution provided laptops for student workers. Though all students at our institution are required to have laptops, the student interns used computers dedicated to cybersecurity training. Dedicating laptops for SOC use helped ensure that all laptops had the correct security settings and network connectivity.

Novacoast hosted the NovaSOC server in its data center. Interns accessed the NovaSOC software through a web browser using an HTTPS connection. Initially, a virtual private network (VPN) was proposed as a second layer of security. The VPN could have required that our institution create specific firewall rules, which would have increased the complexity of network connectivity. However, in the end, the encrypted HTTPS connection was deemed sufficient.

No infrastructure upgrades were required because our facilities met Novacoast's specifications. The only cost to the university for establishing the SOC was the time spent by employees evaluating requirements, signing agreements, and doing similar tasks. No money would change hands between our institution and Novacoast.

3.5 Organizational Commitment

Our institution declared cybersecurity a strategic priority. Everybody involved in the decision-making was supportive of the SOC concept. Faculty members in the cybersecurity degree program were supportive of giving students academic credit for SOC internship work. Executive leadership enthusiastically endorsed the idea. The information technology department saw the SOC as just another program running on campus, and though it did not advocate for the SOC, it did everything necessary to make it work from a technical standpoint.

The university risk management department had concerns. For example, risk management personnel feared that a student might make a mistake causing harm to a company, or a student might release sensitive information. These risks were mitigated in several ways. First, interns would have no direct access to NovaSOC client systems and would therefore be in no position to cause harm. The interns only had restricted access to the NovaSOC SIEM. A memorandum of understanding (MOU) was entered into by both our university and Novacoast. The MOU obligated the university to perform background checks and required that students sign non-disclosure agreements (NDA). While MOUs are typically not legally binding, NDAs are legally binding and our university ensured that background checks were conducted and that every student signed an NDA. Because student interns would have no direct access to Novacoast client systems and were legally obligated to protect sensitive information, we felt that there was minimal risk to our institution.

The human resources department had some issues with the fact that Novacoast required a background check for all SOC interns. Background checks for students are not typically conducted at our institution. According to Novacoast, background checks should only be used to check for convictions that could indicate that a SOC intern could not be trusted with sensitive information—such as a history of financial fraud.

3.6 Employment Arrangement

The employment arrangement warrants consideration. The university demands that all internships that are part of academic credit be paid—an acknowledgment that students should be compensated for the value that they add. However, Novacoast would not be paying the SOC interns. Student interns would use Novacoast's SOC software to analyze alerts for Novacoast's customers, but the interns would only receive and analyze the lowest priority alerts and Novacoast employees would double-check all work. At best, the SOC interns would speed up alert processing by Novacoast employees, but Novacoast perceived little added value from the SOC interns' work. Novacoast's main goal was to help give students real-world experience. A conceptual agreement was made that students who performed well as "Level 1" (unpaid) analysts could at some point be promoted to "Level 2" analysts, thereby becoming true paid Novacoast employees. The timing and terms for student promotion were not clearly defined.

Despite the intrinsic value of the SOC experience for students, the university was still uncomfortable with the work going unpaid. The university had previously obtained grants to improve cybersecurity education with an emphasis on developing a skilled workforce. The grant specifically set aside money for internships. A portion of the grant money was used to pay the SOC interns. Officially, the SOC interns were hired and paid by the university, but they acted as employees of Novacoast.

3.7 Business Development

Novacoast partnered with two regional cybersecurity firms to help sell NovaSOC services. SOC interns would monitor the data for the new Novacoast clients. This seemed like a win for all parties. The cybersecurity businesses in the region would gain revenue with a cut of the NovaSOC fees, Novacoast would gain customers, and the students would gain experience. Unfortunately, business development was slower than anticipated, and we hired more student interns than were needed for the volume of alerts.

3.8 Intern Hiring Process

The SOC internships were advertised like any other on-campus job. The job description was crafted in a way that prioritized students with cybersecurity coursework or experience. The positions were promoted by cybersecurity faculty to their students. Some students not majoring in cybersecurity or a technical degree applied and were accepted because of their interest in cybersecurity. The cybersecurity program could benefit by recruiting students to the cybersecurity major if students had positive experiences as SOC interns.

3.9 Intern Onboarding

In the first week of work in the SOC, students were given training on network security and SIEM tools. The network security training was broadly based on the CompTIA Security+ certification curriculum. The SIEM training covered log analysis, triaging events, and using both Splunk and the NovaSOC software. Analysts were required to use the SIEM tools to analyze a scenario and submit a written report to Novacoast. Interns were not allowed to begin work until passing the report milestone.

3.10 Ongoing Operations

Once training was completed, and the SOC was running, university faculty and staff were needed infrequently. Interns worked shifts during normal business hours between 8 am and 5 pm Monday through Friday. Novacoast monitored their client systems 24x7, so there was no need to have students work late hours or on weekends. Periodic meetings between administrators at our institution and Novacoast were conducted, but neither party raised any significant concerns. There was a sense that student interns were underworked, so a student intern leader developed training systems so that students could continue to sharpen their skills in a virtual environment. Students did not complain about the light workload, likely because they were paid no matter the alert volume.

3.11 Semester Wrap-up

Several student interns wanted to continue working in the SOC at the end of the semester. Because our institution had sufficient funds to support internships, some were allowed to continue. Nevertheless, overall staffing was decreased to align with the expected workload.

The first semester of the SOC was generally considered a success. However, the well of grant funds used to pay student interns would eventually dry up. Novacoast was informed that the SOC could not continue indefinitely under the current arrangement. Soon, student interns would need to be paid by

Novacoast instead of through institutional grant money. Novacoast was optimistic about prospects for continuing business development and the idea of promoting student workers.

4. SOC VALIDATION

Establishing a SOC on a university campus comes with costs, so it is important to validate if the costs justify the benefits to the institution, the students, and other stakeholders.

4.1 Methodology

University administrators and student SOC interns were surveyed at the end of the first semester of the SOC running on campus. A mix of quantitative and free-response questions was included in the questionnaire. Participants were given a chance to discuss their experiences in greater depth via follow-up interviews.

4.2 Analysis of Student Data

A total of 12 students worked in the SOC in the winter 2021 semester. Most of the students were cybersecurity majors, but some students were not and therefore lacked previous cybersecurity coursework. There were two female and ten male SOC interns. Students were sophomores to seniors. Of those students, 5 completed the survey. The means and standard deviations of responses are included in Table 1. The results are sorted by mean from high to low.

Students were asked several open-ended questions, and training was mentioned several times. One student was very positive about the training, saying, "The training we received was done by a professional security analyst. It was hands-on and complete." Another student had mixed feelings about the training, reporting, "Going through more complex test alerts would be great training; other than that the training material was really good it's a lot of information which takes time to go over. In a perfect world I would take unlimited training because it's all so interesting and there's always something new to learn." When asked how Novacoast could have given more support, one student mentioned, "Actually go through a better training program than whatever was given to us." Because students had time on their hands from a low volume of alerts, some asked for additional training resources to better take advantage of their time.

Students were asked about the aspects of working in the SOC that were most helpful for their personal or professional development. One student said, "Learning about the SIEM, learning about the metrics behind how it works, and reading through logs is an opportunity I would not be able to come up with by myself." A different student reported no desire to work in cybersecurity in the long term. Another student was surprised by how few attacks the Novacoast customers were under. A student witnessed the reality of falling victim to phishing attacks, saying, "Literally one of the other intern's computers were targeted by phishing attempts, and they clicked on it on their [school issued] laptop. Who does that???"

We were interested in what coursework might be helpful to prepare students for SOC internships. One student remarked, "No coursework that I have taken to date was necessary for this position." Another student said that introductory networking and network security courses were helpful.

Students were asked what improvements to coursework could be made to better prepare them for working in the SOC. One student wanted more technical courses and fewer business courses. Another student said, "More hands-on, practical applications in our coursework would be helpful."

Prompt	Mean	SD
I was financially compensated appropriately.	6.2	0.8
I was frequently bored while working in the SOC.	5.8	0.8
I would choose to work in the SOC again.	5.8	1.6
I had sufficient support from the university.	5.2	2.2
I had sufficient support from the SOC provider.	5.0	1.7
My previous coursework prepared me to succeed as a SOC employee.	4.6	2.3
I was given sufficient training at the start of my SOC work.	4.4	1.8
Working in the SOC helped prepare me for a career in cybersecurity.	4.2	1.9
My time in the SOC was well spent.	4.2	2.6
I would have worked in the SOC even if I was not paid.	4.0	2.3
Working in the SOC helped me establish career goals for the first time.	4.0	1.0
Working in the SOC helped me change my existing career goals.	4.0	1.0
The work was fulfilling.	3.6	1.5
The work was meaningful.	3.4	1.8
I was frequently challenged by the work.	2.6	2.2
I often felt overwhelmed by the work.	2.4	1.7

Table 1. Means and Standard Deviations of Student Responses (1=Strongly Disagree - 7=Strongly Agree)

The quantitative data indicated that students felt supported by the university and Novacoast. Only one student provided critical feedback on the university's support, saying, "There wasn't really any support from anything. It was a weird brief training that didn't really train anything, and then just threw you in."

Students were asked about support from Novacoast. One student enjoyed "[t]heir willingness to explain everything to someone who knows basically nothing." One student would have appreciated more check-ins, saying, "After training, there was no contact with anyone from [Novacoast]." Students generally would have preferred more communication and more guidance on using the SIEM.

4.3 Analysis of Administrator Data

Two administrators (both male) completed the survey, and one participated in follow-up interviews. Means and standard deviations of survey responses are included in Table 2.

Administrators were asked about the challenges that had to be overcome to create the SOC on campus. They listed funding for student positions, student capacity planning, and issues scheduling student work times with Novacoast. In what is hopefully a unique time in history, one administrator reported that "State and university guidelines related to the COVID-19

pandemic presented some challenges." For example, at times the university abruptly forbade visitors on campus, which made meeting with internal and external stakeholders challenging. Novacoast's training had to be delivered remotely instead of face-to-face as would have been preferred.

Prompt	Mean	SD
The SOC supports the university's mission.	6.5	0.7
The SOC has been a success.	6.0	0.0
Other universities would benefit from establishing a SOC.	5.5	0.7
The SOC is a strategic priority of the university.	5.0	0.0
There were significant organizational challenges to overcome to establish the SOC.	4.5	0.7
There were significant technical challenges to overcome to establish the SOC.	3.0	1.4
People at the university understand the work done at the SOC.	2.5	0.7

Table 2. Means and Standard Deviations of Administrator Responses (1=Strongly Disagree - 7=Strongly Agree)

Administrators reported several successes. Just making the SOC happen was a success, according to one administrator. Helping students gain experience was also reported. One administrator said, "We have developed a strong and hopefully long-term relationship with a Cybersecurity company that is looking to expand and increase its workforce and is willing to engage with students to help prepare them for cyber careers."

Administrators were asked to give their vision for the SOC going forward. One administrator wants a "[f]ully entrenched self-sustaining capability within the [institution] that provides a conveyor belt path of internships for academic and non-academic students. Students start as level 1 student analysts, and after one year of demonstrated success, those students are hired as interns with Novacoast and provided the opportunity to perform higher-level SOC analyst functions. Upon graduation or completion of [institution training] courses, students have both the knowledge, and experience to become successful cyber professionals."

5. DISCUSSION

The general sentiment from students and administrators is that the SOC has been a success, but there are areas for improvement. This section summarizes key lessons learned and provides guidance for others seeking to develop similar models.

5.1 Training

The students had large disparities in previous coursework and experience when starting internships in the SOC, but all were given the same training. One student reported that the training was "hands-on and complete," but another student reported wanting to "go through a better training program than whatever was given to us." A large amount of training content was given in a short amount of time. That training likely filled in some knowledge gaps for the more experienced students but may have overwhelmed the less experienced students. Additional assessment at the end of training could have identified those individuals who felt underprepared at training completion.

The data on training and coursework imply that while university coursework teaches cybersecurity fundamentals, the training provided at the beginning of the internship was sufficient to prepare students for SOC work. Therefore, these kinds of internships should not be reserved for students who have already completed several cybersecurity courses, with the caveat that differentiated training be given based on skill level.

5.2 Aligning Incentives

Because Novacoast did not pay the student employees, there may have been less incentive for Novacoast to ensure that interns were engaged and productive. It was not initially clear to the university that only data from new Novacoast customers in the region would be sent to the campus SOC. While this arrangement could have resulted in a win-win scenario with Novacoast gaining new customers and students gaining real-world experience, the reality was that business development lagged SOC staffing. Overall, the SOC employed many more students than necessary for the amount of data that needed to be analyzed. The university hoped that Novacoast could hire some students as level 2 analysts, but that prospect in the short term seems unrealistic unless business development accelerates quickly.

From an institutional perspective, the SOC helped the administrator in the continuing education department achieve the mandate of increasing skills and employment opportunities. Faculty on the other side of the university are tasked with teaching as the primary focus, research as a secondary focus, and service third. Because helping create a SOC would fall under service (the least emphasized area of a faculty's responsibilities), it is not clear if there would have been sufficient incentives for the faculty to do the work necessary to establish the SOC without support from the continuing education department. Institutions must ensure that faculty, staff, and administrators are properly incentivized to embark on innovative endeavors.

5.3 Financial Sustainability

The on-campus SOC cannot be sustained indefinitely with its present financial model. Grant money funded the current internships, but grant money is limited, and other initiatives compete for resources. For the SOC to be sustainable, students may need to work unpaid until promotion to Novacoast-paid employees. While students might benefit in the long-term from a short-term unpaid position, it feels morally wrong to ask students to work for free when their education costs continue to increase. We do not blame Novacoast for this problem. We are grateful that Novacoast came to us and offered to give students experience. This desire to help build peoples' resumes is in contrast to the employers who advertise entry-level jobs that require 3-5 years of relevant experience. Overall, the cybersecurity industry must find a way for entry-level employees to add real value.

5.4 Support and Interaction

Checking in with the students periodically could have helped identify those who felt like they needed more support. Because nobody heard complaints during the semester, we assumed that everything was going well for the students. A plan for checking

in periodically should have been agreed upon between our institution and Novacoast.

Because the students operated relatively independently with less interaction with the university and Novacoast, they did not have opportunities to learn from more knowledgeable others—a critical component for developing skills (Guile & Griffiths, 2001). Efforts should be taken to ensure that student interns are learning from experienced professionals, not just the work tasks. Being a remote site made interactions at the water cooler impossible. Novacoast employees could not simply poke their heads in the office to check in on students. Formal arrangements for both professional and social interaction between the student interns and Novacoast employees should have been planned.

5.5 Going Forward

No changes to facilities, network connectivity, or legal agreements are needed at this point. However, several changes are expected going forward. In the short term, the university will modify the program to calibrate staffing with the expected alert volume more tightly. The university is working with local institutions to recommend security monitoring services but ultimately has no control over business development and alert volume. In the medium term, it is hoped that formal pathways for student promotion to Novacoast-paid positions can be established. In the long term, it is hoped that additional industry partnerships can be established with similar internship models. Financial sustainability will be a key factor in all program changes.

6. CONCLUSIONS

The cybersecurity field needs people with skills and experience. Partnering with a company to provide work opportunities on campus helped our institution prepare students for successful cybersecurity careers. Institutions seeking to establish similar models should engage stakeholders in their academic institutions early in the discussions around creating partnerships with private companies. Institutions should also ensure that incentives are properly aligned so that the partnership adds value to all parties. Understanding the motivations and benefits of industry partners and university employees is essential. Discussions about long-term sustainability should happen early in the process. While our institution was glad that it pursued a SOC using grant funding to pay students, it is recognized that this is a short-term solution. Though imperfect, we consider the endeavor to bring a SOC on campus a success. As Confucius said, "Better a diamond with a flaw than a pebble without" (Singh, 2006, p. 223). We are optimistic about the future of the SOC and the benefits it provides.

7. ACKNOWLEDGEMENTS

We would like to thank Novacoast for helping give students an opportunity to gain skills and experience while pursuing their degrees.

8. REFERENCES

Becker, J. D., & Brown, C. V. (2000). Industry/Academic Partnerships in Information Systems and Technology. *AMCIS 2000 Proceedings*, 262.

Ben Fredj, O., Mihoub, A., Krichen, M., Cheikhrouhou, O., & Derhab, A. (2020). CyberSecurity Attack Prediction: A Deep Learning Approach. *13th International Conference on Security of Information and Networks*, 1-6. https://doi.org/10.1145/3433174.3433614

Bhatt, S., Manadhata, P., & Zomlot, L. (2014). The Operational Role of Security Information and Event Management Systems. *IEEE Security & Privacy*, 12(5), 35-41.

Guile, D., & Griffiths, T. (2001). Learning Through Work Experience. *Journal of Education and Work*, 14(1), 113-131. https://doi.org/10.1080/13639080020028738

Kelley, D., & Moritz, R. (2006). Best Practices for Building a Security Operations Center. *Information Systems Security*, 14(6), 27-32.

Lave, J., & Wenger, E. (1991). *Situated learning: Legitimate Peripheral Participation*. Cambridge University Press.

Legier, J., & Soares, A. (2014). IT Educational Experience and Workforce Development for Information Systems and Technology Students. *Information Systems Education Journal*, 12(6), 71-82.

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (NIST CSWP 04162018; p. NIST CSWP 04162018). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

Payne, B., Mayes, L., Paredes, T., Smith, E., Wu, H., & Xin, C. (2020). Applying High Impact Practices in an Interdisciplinary Cybersecurity Program. *Journal of Cybersecurity Education, Research and Practice*, 2020(2), 1-26.

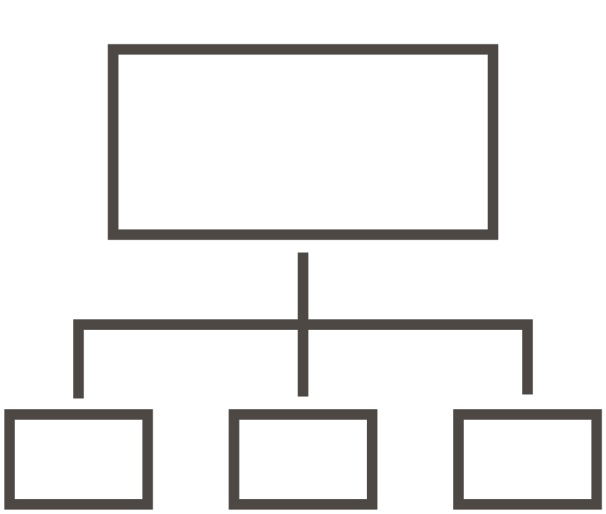
Pittenger, K. (2021). Virtual Internships—A New Reality. *Developments in Business Simulation and Experiential Learning*, 48, 149-152.

Singh, M. P. (2006). *Quote, Unquote: A Handbook of Famous Quotations*. Lotus Press.

Stoker, G., Clark, U., Vanajakumari, M., & Wetherill, W. (2021). Building a Cybersecurity Apprenticeship Program: Early-Stage Success and Some Lessons Learned. *Information Systems Education Journal*, 19(2), 35-44.

AUTHOR BIOGRAPHY

Jim Marquardson is an associate professor of information assurance and cyber defense in the College of Business at Northern Michigan University. His Ph.D. in Management Information Systems is from the University of Arizona. Professor Marquardson's research focuses on human-computer interaction, information security behavior, and persuasive technology. His research has been published in *Interacting with Computers*, *Decision Support Systems*, and the *Information Systems Education Journal*.



Information Systems & Computing Academic Professionals

Education Special Interest Group

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