THE CISO ACADEMY

Researching New Ways to Build a Cybersecurity Workforce

Pamela D. Curtis, Summer Craze Fowler, David Tobar, and David Ulicne

December 2016

Organizations across the world face the increasing challenge of attracting and retaining a skilled cybersecurity workforce. That's why the CERT Division at Carnegie Mellon's Software Engineering Institute has been researching the best methods and approaches for cyber workforce development. As part of this research, CERT cybersecurity experts often work with organizations to understand workforce development needs as well as implementation issues and opportunities. One such organization is the United States Postal Service (USPS).

Being one of the largest organizations in the country, the USPS is not immune to the challenge of establishing effective cybersecurity capabilities. Over the last few years, the USPS Corporate Information Security Office (CISO) assessed its ability to prevent and respond to cybersecurity threats. It found, like many large organizations, that it was unable to keep pace with the fast-growing cybersecurity landscape. To strengthen its security culture and support its cybersecurity mission, the Postal Service committed to developing its workforce by forming the CISO Academy.

In this paper, we describe the joint project that a Postal Service and SEI team conducted to develop the academy's curriculum, the need that led to its formation, the experiences of its first graduating class members, and next steps in this groundbreaking approach to tackling cybersecurity workforce development.

A Weakness Is Revealed

In the fall of 2014, the Postal Service fell victim to a sophisticated and extensive attack of its networks and systems. The attack compromised the personally identifiable information (PII) of the more than 800,000 Postal Service employees and the PII of more than two million of its customers. The attack was thoroughly investigated by the Postal Service, private sector specialists, and federal agencies. The investigation's conclusions included that the Postal Service information security (IS) unit was understaffed and underskilled. Faced with insufficient IS capability, it was difficult for the Postal Service to respond to the attack. The Postal Service recognized it needed to better protect its data from future attacks, prevent similar breaches, and quickly respond to threats. Improved training for CISO staff would be key.

A Collaboration Is Strengthened and a Solution Takes Shape

Since 2011, the Postal Service has engaged Carnegie Mellon University's Software Engineering Institute to provide cybersecurity expertise in incident response, workforce development, operational resilience improvement, and other cybersecurity areas. For example, the SEI and Postal Service collaborated to build and implement a cybersecurity technical strategy and roadmap that focused on operational resilience as defined in the CERT Resilience Management Model (CERT-RMM) [Caralli 2010]. This

approach now enables the Postal Service to better execute its mission during and after disruptive events such as the 2014 data breach and provides valuable feedback to SEI researchers.

After the data breach, the Postal Service received funding to increase its IS staff and improve its capabilities. Given the success of past collaborations with the SEI, it was natural for the Postal Service and the SEI to work together again to address the weaknesses the Postal Service data breach exposed and provide new field experience to enhance CERT cyber workforce development research. Acting Chief Information Security Officer (CISO) of the Postal Service Greg Crabb reached out to the SEI to discuss his training needs and brainstorm solutions. Crabb envisioned forming a world-class, boot-camp style program that immerses its students in intensive cybersecurity training for 9 to 12 weeks. Working together, the SEI and the Postal Service created a team that subsequently developed the formal program known as the CISO Academy.

The SEI's more than 30 years of cybersecurity experience enabled it to help the Postal Service form, launch, and pilot the CISO Academy. As a federally funded research and development center, the SEI is uniquely positioned to provide objective expertise and use this experience of creating the academy to enhance its research agenda. The SEI's access to Carnegie Mellon University (CMU) resources in curriculum development and training best practices provided the skill and knowledge to enable the USPS team to form the academy's curriculum.

In early 2016, the SEI and Postal Service team delivered a pilot offering of the CISO Academy program to a group of students and identified and captured measures based on that delivery. The team incorporated lessons learned into cybersecurity training and best practices for ultimate use by the U.S. Department of Defense.

Once the pilot program was ready, Crabb named 20 Postal Service staff members to receive training, invited them to enroll in the academy, and used contractors for staff augmentation while students attended the program. To ensure that the Postal Service benefited from the training program, his plans required that all students commit to working for the Postal Service for two years following graduation.

The CISO Academy Opens

The pilot offering of the program included courses based on material provided by the DHS, including the Federal Virtual Training Environment (FedVTE)[1]; Franklin Covey; and the SEI, including courses that are part of the CERT Simulation, Training, and Exercise Platform (STEPfwd).[2]

---

1 FedVTE offers cybersecurity courses at no cost to federal government personnel and U.S. veterans.

2 STEPfwd combines online cybersecurity courses with virtual labs.

In their studies, students had learning experiences ranging from in-person sessions to virtual courses, labs, and group cyber exercises, and they completed a core set of courses:

- Franklin Covey's *The Speed of Trust*
- a cyber security overview
- an insider threat overview

Specialty courses, based on the roles of the students, were divided into two tracks: a program manager track and a technical staff track. Tracks covered the following topics:

Program Manager Track

- CSIRT/SOC development
- Insider threat program development
- Cyber risk management/assessment
- Cyber policy
- Supply chain risk management
- Cybersecurity metrics
- Enterprise/software architecture
- Software assurance
- Security requirements engineering

Technical Staff Track

- Network security
- Systems administration
- Incident response
- Digital forensics
- Cryptography
- Vulnerability assessment
- Operating system security
- Network monitoring
- Penetration testing

During their 12 weeks at the CISO Academy, students had 2 weeks on their own. One week was designated for independent study and the other allowed them to check in on their jobs. During independent study, students selected and completed FedVTE or STEPfwd courses related to their job responsibilities.

The academy's mentorship program allowed students to ask questions about courses and applying their new knowledge to their daily roles. The last week of study included capstone exercises tailored for either the program manager or technical staff track. In each exercise, students used their newfound knowledge, skills, and abilities to react to a simulated event. CISO Academy faculty used these exercises to evaluate how prepared each student was to return to work and support the Postal Service cybersecurity mission. At the end of their course work, many students took advantage of their training to also take and pass relevant accredited industry certification exams.

A New Workforce Is Unleashed (the Students Graduate)

All 20 students candidates successfully completed the academy's first program offering, and on May 19, 2016, the students candidates graduated. Prior to graduation, they elected a fellow student who most exemplified the CISO Academy values and goals. At graduation, this model student gave a commencement speech, and several other students received the "Above and Beyond Award" for voluntarily taking extra FedVTE or STEPfwrd courses that were not part of the academy's formal curriculum.

In the weeks after graduation, students' managers helped them transition back to their Postal Service jobs. Some students returned to different jobs because their newly expanded skills qualified them to work in positions with expanded responsibilities. The SEI is now working with the Postal Service to

learn how the training affects the performance of the academy attendees and, in turn, the cybersecurity posture of the organization.

Evaluation and Improvement Begin

After completing each course, students provided feedback; based on this feedback and observations of academy leaders, changes were planned for the CISO Academy program. Student feedback was used to improve the program and was also fed back into the ongoing data collection that supports cyber workforce development research at the SEI. These improvements include the following:

- having mentors attend the orientation in person and meet the students face-to-face
- refining the curriculum (e.g., align it further with the National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework [NICE 2016])
- adding additional electives to the curriculum
- building more free time into the schedule to result in a 14-week-long program with 2 free weeks
- tailoring the curriculum according to the qualifications, experience, and professional development needs of the students (e.g., add more challenging courses)
- assessing students' progress frequently
- customizing courses to relate to Postal Service tools and situations
- increasing interaction of students between the two tracks

The second class of the CISO Academy will graduate in Spring 2017 and will include new hires and employees from Postal Service departments who applied to enroll in the CISO Academy. Like the first graduating class, new hires trained at the academy will be required to agree to a minimum two-year commitment with the Postal Service.

The Challenge Continues

Graduates of the academy are expected to extend their professional development through a formal continuing education program that includes hot topic workshops and cybersecurity exercises. Successful graduates can become mentors to future academy graduates. The SEI and Postal Service team will enhance the program as it analyzes its impact. The SEI will look for opportunities to work with other organiations to gather data and try new ideas as part of its research.

After graduating one class and with future offerings being planned, the Postal Service has made solid progress toward its goal of ensuring that members of the CISO organization have the necessary skills to create the state-of-the-art cybersecurity workforce needed to support the Postal Service cybersecurity mission.

The results of Postal Service hiring practices, the CISO Academy, and mentoring program will be interesting to SEI researchers as they continue to study the landscape and security trends to form practices and approaches to help organizations prepare a robust cyber workforce.

References

[Caralli 2010]
Caralli, Richard A.; Allen, Julia H.; & White, David W. CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience. Addison-Wesley Professional. November 2010. http://www.informit.com/store/cert-resilience-management-model-cert-rmm-a-maturity-9780321712431

[NICE 2016]
National Initiative for Cybersecurity Education, National Cybersecurity Workforce Framework. *National Institute of Standards and Technology*. http://csrc.nist.gov/nice/framework/

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org
Email: info@sei.cmu.edu

This material is based upon work funded and supported by United States Postal Service under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM-0004516