Cybersecurity for Leadership (C4L)

Cybersecurity training for decision makers

CENTER FOR APPLIED CYBERSECURITY RESEARCH

Innovation Center
2719 E. 10th Street, Suite 231
Bloomington, IN 47408
Phone: 812.856.0458
Fax: 812.856.7400

Cybersecurity is not a solved problem. Organizations are tasked with defending against criminals and nation-state actors. Most technology is fundamentally insecure and cybersecurity is much more than a technical challenge. As a field of practice, cybersecurity is immature and expertise is hard to find. All these things make organizational leaders' jobs challenging.

Introducing C4L: Cybersecurity for Leadership

The Center for Applied Cybersecurity Research (CACR) created C4L targeted to both non-cybersecurity and cybersecurity leaders to address these issues and more.

> After piloting the C4L Bootcamp with public and private institutions, we asked, **"Would you recommend C4L to other organizations?"** One chief of HR information systems said:
>
> *Hell yes, I will for sure.*

About the curriculum and Bootcamp. The C4L curriculum begins with a half-day bootcamp. It provides practical tools to help organizational leaders play an effective role in cybersecurity oversight.

The Bootcamp includes explicit detail on what leaders must do (and avoid) to establish a competent cybersecurity program and organizational culture conducive to reasonable security. The Bootcamp curriculum focuses on decision-making, strategy, communication, and cybersecurity programmatics. It features two first-of-their-kind knowledge products. Its Programmatic Module covers Mission Alignment, Governance, Resourcing, and Controls. These four Pillars of the Trusted CI Framework (see trustedci.org/framework) set out the foundational requirements for any competent cybersecurity program. Its Strategy Module introduces your organization to CACR's Information Security Practice Principles (see cacr.iu.edu/principles). These seven easy-to-understand concepts give all organizational personnel a common language and support leaders in asking the right questions and making fundamental decisions about cybersecurity investment.

Intermediate and advanced training packages are available for organizations who desire more in-depth training.

C4L Bootcamp: half-day in three modules

Module 1

Introduction

Framing the challenge
- What is cybersecurity?
- What do leaders do?

Module 2

Trusted CI Framework
- Mission alignment
- Governance
- Resourcing
- Controls

Module 3

Information Security Practice Principles
- Communication
- Decision-making
- Strategy

O'REILLY

Security from First Principles

Craig Jackson, Scott Russell & Susan Sons

REPORT

For more information, please contact **cacr@iu.edu** or visit **go.iu.edu/40Sm**

Upon completing the C4L Bootcamp, participants will:

- Have new perspectives on the role of organizational leaders in dealing with cybersecurity.
- Understand fundamentals and common issues with having an organized programmatic approach to cybersecurity.
- Have a new set of concepts and terms you can use, regardless of cyber expertise, in communicating and making decisions.
- Be better able to evaluate cybersecurity information, news, products, assertions, and requests.
- Have a greater understanding of your colleagues' perspectives, concerns, and roles regarding cybersecurity.

Training formats and tech requirements. Our expert instructors use a blend of presentation, Q&A, and guided activities—all live—to engage participants. Our training approach and activities are based on research-proven methodologies and expert guidance.

We offer C4L both in person and virtually.

- In-person classroom presentations and exercises can take place at CACR or your location. (Requires A/V capabilities and writing surfaces for participants.) Benefits include greater opportunities for interaction between participants and instructors, with more flexibility for conducting activities.
- Virtual interactive presentations and exercises can be scheduled at your convenience. (Requires participant access to a computer with a working video camera and microphone.) We can use Indiana University's licensed Zoom instance or the video teleconferencing service of your choice. Benefits include reduced cost and easy accommodation of distributed participants.

Preparation. While our curriculum is relevant to all contemporary organizations, we collect inputs (through brief interviews or questionnaires) from participating organizations to help our instructors tailor the curriculum to customer needs, mission, and cybersecurity maturity.

Recommended participants. Organizations that get the most out of C4L take this as an opportunity to get key people in the same conversation, speaking the same language. We recommend including organizational executive leadership teams, technology leaders, technologists, and cybersecurity personnel.

Continuing education and workforce development. We provide all the documentation needed for participants to attain continuing education credits. Our training is mapped to NICE Framework (nist.gov/itl/applied-cybersecurity/nice) specialty areas, particularly those under the OVERSEE and GOVERN Cybersecurity Work Category.

Meet your instructors

Craig Jackson is program director at CACR. He leads collaborative work with the national security community, as well as interdisciplinary assessment and guidance teams for the NSF Cybersecurity Center of Excellence. He is the chief architect of the Trusted CI Framework and has served as temporary faculty at Naval Surface Warfare Center Crane. Craig is a graduate of the IU Maurer School of Law, IU School of Education, and Washington University in St. Louis.

Scott Russell is a senior policy analyst with CACR, where his work focuses on the improvement of cybersecurity and privacy policy. He is the program lead for the Trusted CI Framework, a co-author of *Security from First Principles: A Practical Guide to the Information Security Practice Principles*, and served as temporary faculty at Naval Surface Warfare Center Crane. He received his B.A. in Computer Science and History from the University of Virginia, J.D. from Indiana University, interned at MITRE, and served as a postdoctoral fellow at CACR.