A Strategy for Collaboration between Information Security Education, Operations, and Research at Indiana University

Deliberative Draft
May 27th, 2021

Von Welch
Executive Director for Cybersecurity Innovation, Indiana University (vwelch@iu.edu)

http://hdl.handle.net/2022/26458

Abstract

Indiana University has built a unique combination of operational, research, and educational information security endeavors. However, there has not been a sustained collaborative effort between these endeavors. This document will mature through discussions to set out a strategy for how IU's unique applied information security capabilities should work in collaboration with its education and research programs to coherently collaborate to maximize IU's collective impact on IU students, IU researchers, the state of Indiana, and the nation.

IT as a Catalyst for Cybersecurity Research and Education

Indiana University (IU) has built a world-class information technology (IT) environment in support of its mission of excellence in education and research. The importance of this IT environment is captured in a quote from President Michael McRobbie, who was Indiana University's first Vice President for Information Technology, which opens the last two IU strategic plans for IT: *"Information Technology is today one of the most critical tools in higher education. It permeates every aspect of a University from the first contact a student has with its Web site through the myriad systems that manage and provide access to its information..." (ep.iu.edu)*

IU has developed a strong operational information security capability to secure this IT environment. Additionally, IU innovates in information security at the national scale through its leadership of several applied information security organizations: the Center for Applied Cybersecurity Research (CACR/cacr.iu.edu), the Research and Education Networks Information Sharing and Analysis Center (REN-ISAC/ren-isac.net), the NSF Cybersecurity Center of Excellence (Trusted CI/trustedci.org), the OmniSOC (omnisoc.iu.edu), and the ResearchSOC (researchsoc.iu.edu). In aggregate, IU's operational information security capability combined with these applied information security organizations represent an information security endeavor that goes well beyond IU’s peers and uniquely position IU as the higher education leader in information security.

In line with IU’s mission and in parallel to its operational information security activities, IU has developed educational and research programs in information security, for example, the M.S. in Cybersecurity Risk Management, the Master of Science in Secure Computing, the B.S. in Cybersecurity and Global Policy, and the Ostrom Workshop Program on Governance of Internet & Cybersecurity. While there are examples of collaborations between IU’s educational, operational, and research information security endeavors, there has not been a strategic collaborative effort between them. The reasons for these gaps are structural as IU’s organizational and financial model incentivizes and rewards performance within functional groups rather than across groups. Deep and sustained collaborations do not have natural structures, and good-willed champions have to carve a path and sustaining mechanisms outside of the institution’s deep culture.

This document will mature through discussions to set out *a strategy for how IU’s unique applied information security capabilities should work in collaboration with its education and research programs to coherently collaborate to maximize IU’s collective impact on IU students, IU researchers, the state of Indiana, and the nation*.

This strategy does not propose to change the governance of information security entities or to unilaterally change agreements that IU or any of the relevant organizations it leads (the REN-ISAC, NSF CCoE, OmniSOC, or ResearchSOC) may have made with external entities barring further discussion with those entities. Instead, the aim of the strategy is to serve as an agreement as to what IU information security entities will do in collaboration and to allow others in the IU community to understand the context of those collaborations and the envisioned future.

The document starts by laying out strategic principles for the collaboration to define the collaboration’s goals. That is followed by a description of the status of current progress towards these goals as of the time of this document’s creation in mid-2019. It concludes with prioritized recommendations to advance IU towards the goals.

A note on terminology: this document uses the term “information security” where one could also use “cybersecurity” or “computer security” and does not attempt to draw any distinction between these terms.

Principles of IU’s Information Security Collaboration

The following principles serve to define the goals of the collaboration between IU’s applied, educational, and research endeavors:

Principle 1: IU information security operations should catalyze research through policy-compliant access to infrastructure and data.

Discussion: Information security research has a documented need for access to real world data and infrastructure to perform research and to evaluate research results (e.g., [1]). Data from IU internal operations can provide large and valuable data to further the institution's research mission. Access to data and infrastructure must be done in a manner that absolutely protects the privacy of the IU community and does not compromise the integrity and availability of the operations. Additionally, similar approaches to the use of data could also be formally adopted by IU and its partner institutions for even larger data resources for research at IU and with partner institutions.

The REN-ISAC member institutions and community are not ready to participate with their data at this time, and those datasets are of less interest than other IU and partner data.

Status: Currently sharing is done on an unadvertised, ad hoc basis when requested by researchers, with six such requests over the past three years at IU. The OmniSOC and ResearchSOC projects are working in collaboration to make their data available to their constituencies in 2020 (e.g., [2]).

Possible Next Steps:

1. OmniSOC and ResearchSOC should complete their current projects to make data available.
2. IU should undertake a program to allow operational data and infrastructure, from IU and partners where appropriate agreements exist, to catalyze research.
3. This program should be documented and advertised to researchers and serve as a tool by academic departments to recruit students and faculty.
4. IU's operational information security program and applied information security organizations should offer sabbatical opportunities to have researchers spend time embedded in their organizations to conduct research.
5. IU should offer simulated data for AI training and education to reduce the need for real data.

Principle 2: IU Information security operations and applied research should enhance education through real-world learning and workforce development opportunities.

Discussion: Collaboration between IU's educational and operational information security endeavors holds the promise of unique educational offerings that prepare its graduates well and provides IU's educational programs with a competitive advantage in attracting students. Stronger ties with IU's information security alumni will also serve IU well by building a network of collaborators for competitive funding situations.

Status: Several instances of this exist: (1) the OmniSOC operated an internship program in the Summer of 2019 [3]; (2) CACR collaborates with Maurer to provide a required work experience for 2-4 JD students each year that are earning a certificate in either Cybersecurity Law and Policy or Information Privacy Law and Policy; and (3) CACR hosts two annual CyberCamps, one for high schoolers and one in collaboration with CEW&T for non-STEM undergraduates. Other collaborations for IU students are ad hoc.

Possible Next Steps:

1. IU should aggressively pursue a summer student intern programs drawing on OmniSOC partners and NSF REU grants.
2. IU should aggressively pursue an organized academic year internship program providing IU and partner institution students with the opportunity to gain hands-on experience.
3. IU should provide infrastructure for education that simulates real-world infrastructure and data (for example, a cyberrange or a student-run SOC).
4. IU should maintain a list of operational information security staff willing to lecture in information classes on relevant topics.

Principle 3: IU should translate research into practice within the operational information security infrastructure.

Discussion: Application of research can improve IU's operational information security capabilities. There also exists, for example through NSF's Transition to Practice Efforts, funding to catalyze translation of research.

Status: CACR has undertaken a pair of workshops through the NSF Cybersecurity Center of Excellence and conducted a pilot in collaboration with the OmniSOC and Research Technologies to work with Dr. Jay Wang of RIT on prototyping his AI/ML research [2].

Possible Next Steps:

1. IU should actively advertise its willingness to experiment with research results in its information security environments.

Principle 4: IU should provide a world-class environment for research with compliance and other information security requirements.

Discussion: IU's main source of external research funding is NIH, which often brings compliance requirements in terms of HIPAA, FISMA, 21 CFR Part 11, etc. IU also sees funding with NIST 800-171 requirements and other data use agreements. Application of IU's applied information security acumen allows this research to be accomplished both efficiently and in a manner that manages institutional risk.

Status: HIPAA is fairly well supported, with maturation in process, in a distributed manner between the Offices of the Vice President for IT, Vice President for Research, Vice President and General Counsel, and the School of Medicine. CACR, through its new role in supporting the Executive Director for Cybersecurity Innovation (EDCI) and in collaboration with other entities at IU, is prototyping the

SecureMyResearch consultation service to support research involving NIST 800-171 and other forms of sensitive data, and with other cybersecurity needs.

Possible Next Steps:

1. The Chief Privacy Officer should continue to lead IU in developing a comprehensive plan to address HIPAA and emerging views of Privacy in operational use and legal compliance (e.g., GDPR).
2. CACR/EDCI, in close collaboration with Research Technologies and IU information security and data leadership, should prototype environments for NIST 800-171/CUI to inform broader efforts across IU.
3. CACR/EDCI should continue the SecureMyResearch consulting pilot to provide researchers, ORA, and other IU units with guidance on meeting compliance needs and measuring effectiveness of this pilot to determine a long-term path.

Principle 5: IU should leverage its combination of information security education, operations, and research.

Discussion: With IU's unique combination of applied, educational, and research capabilities, it is uniquely positioned to compete for funding and other opportunities if it can effectively coordinate their strengths. This coordination has to be efficient to meet the short timelines required for some opportunities and must heed limitations from IU's obligations for privacy and operational security, and constraints that stem from its agreement with its partner organizations.

Status: While progress has been made, there are cultural and administrative barriers to this sort of collaboration.

Possible Next Steps:

1. IU should develop a list of funding opportunities and agencies that would make good targets for its combination of interdisciplinary and translational strengths.
2. IU should develop methods for internal communication among its information security entities such that strengths from all those entities are leveraged in external relationships.
3. IU should develop agreements among its information security entities that encourage collaboration. For example, agreements on sharing of indirect returns on grants.

Acknowledgments and To Comment on This Document

Numerous colleagues at Indiana University contributed to this document directly through comments on the document or indirectly through conversations. While the opinions expressed do not necessarily reflect the views of these individuals, we thank them for their contributions. These colleagues at IU include: Isak Nti Asare, Jean Camp, Sara Chambers, Tom Davis, Esfandiar Haghverdi, Apu Kapadia, Andrew Korty, Rob Lowden, Asaf Lubin, Kim Milford, Sagar Samtani, Scott Shackleford, Anurag Shankar, Joe Tomain, XiaoFeng Wang, Brad Wheeler. Thank you to the IT Communication Office for their editorial assistance.

The Executive Director for Cybersecurity Innovation is supported by the IU Office of the Vice President for Information Technology and the IU Office of the Vice President for Research.

To comment on this document directly, please contact Von Welch, Executive Director for Cybersecurity Innovation at Indiana University at vwelch@iu.edu.

References

[1] Jean Camp, Lorrie Cranor, Nick Feamster, Joan Feigenbaum,Stephanie Forrest, Dave Kotz, Wenke Lee, Patrick Lincoln, Vern Paxson, Mike Reiter, Ron Rivest, William Sanders, Stefan Savage, Sean Smith, Eugene Spafford, Sal Stolfo, “Data for Cybersecurity Research: Process and Wish List,” Jun. 2009 [Online]. Available: https://www.researchgate.net/publication/255960171_Data_for_Cybersecurity_Research_Process_and_Wish_List. [Accessed: 27-Aug-2019]

[2] S. J. Yang, A. Okutan, G. Werner, S.-H. Su, A. Goel, and N. D. Cahill, “Near Real-time Learning and Extraction of Attack Models from Intrusion Alerts,” *arXiv [cs.CR]*, 25-Mar-2021 [Online]. Available: http://arxiv.org/abs/2103.13902

[3] “Inaugural Internship Program Changes Students’ Futures -OmniSOC.” [Online]. Available: https://omnisoc.iu.edu/inaugural-internship-program-changes-students-futures/. [Accessed: 25-May-2021]