



# NATIONAL CYBERSECURITY INSTITUTE JOURNAL

Volume 2, No. 3



© Excelsior College, 2015

ISSN 2375-592X

National Cybersecurity Institute | 2000 M Street, Suite 500 | Washington, D.C. 20036  
Excelsior College | 7 Columbia Circle | Albany, NY 12203-5159

# NATIONAL CYBERSECURITY INSTITUTE JOURNAL

---

Volume 2, No. 3

## FOUNDING EDITOR IN CHIEF

---

Jane LeClair, EdD,  
National Cybersecurity Institute at Excelsior College

## ASSOCIATE EDITORS

---

Nadine H. Alami, Doctoral Candidate,  
National Cybersecurity Institute at Excelsior College  
Michael Tu, PhD, Purdue University

**5. Project-based Curricular Service Learning for Cybersecurity Education**

Ping Wang

---

**13. A Probabilistic Framework for Quantifying Mixed Uncertainties in Cyber Attacker Payoffs**

Samrat Chatterjee  
Ramakrishna Tipireddy  
Matthew Oster  
Mahantesh Halappanavar

---

**25. Creating New Private-Public Partnerships in Cybersecurity**

Chris Golden

---

**31. Evolution of Information Security Issues in Small Businesses**

Debasis Bhattacharya  
Debra A. Nakama

---

**45. Hybrid Implementation of Flipped Classroom Approach to Cybersecurity Education**

Aparicio Carranza  
Casimer DeCusatis

---

**55. Malware Fingerprinting: Analysis of Tool Marks and Other Characteristics of Windows Malware**

Sean McVey

---

**65. Strengthening Cyber Incident Response Capabilities Through Education and Training in the Incident Command System**

Austen D. Givens

## EDITORIAL BOARD

---

### FOUNDING EDITOR IN CHIEF

Jane LeClair, EdD,  
National Cybersecurity Institute at Excelsior College

### ASSOCIATE EDITORS

Nadine H. Alami, Doctoral Candidate,  
National Cybersecurity Institute at Excelsior College  
Michael Tu, PhD, Purdue University

## PEER REVIEWERS

---

The *National Cybersecurity Institute Journal* gratefully acknowledges the reviewers who have provided valuable service to the work of the journal:

### PEER REVIEWERS

Mohammed A. Abdallah, PhD,  
Excelsior College/State University of NY  
James Antonakos, MS,  
Broome Community College/Excelsior College  
Barbara Ciaramitaro, PhD  
Excelsior College/Walsh College  
Kenneth Desforges, MSc, Excelsior College  
Amelia Estwick, PhD, Excelsior College

Ron Marzitelli, MS, Excelsior College  
Kris Monroe, AOS, Ithaca College  
Kevin Newmeyer, PhD, National Cybersecurity Institute Fellow  
Charles Parker, Doctoral Candidate, Ciena Healthcare  
Denise Pheils, PhD, Excelsior College  
Lifang Shih, PhD, Excelsior College  
Michael A. Silas, PhD, Excelsior College/Courage Services  
Michael Tu, PhD, Purdue University

## NATIONAL CYBERSECURITY INSTITUTE JOURNAL

---

The National Cybersecurity Institute at Excelsior College is a research center based in Washington, DC, dedicated to increasing knowledge of the cybersecurity discipline and its workforce demands. Published three times a year, the peer-reviewed National Cybersecurity Institute Journal covers topics that appeal to a broad readership within the cybersecurity discipline, with a particular focus

on education, training, and workforce development. The manuscripts submitted to the journal are reviewed for their contribution to the advancement of applied research in the area of cybersecurity.

Submission guidelines for authors can be found at [www.nationalcybersecurityinstitute.org/journal/](http://www.nationalcybersecurityinstitute.org/journal/).

## FROM THE EDITOR

---

Welcome to the third issue in Volume 2 of the National Cybersecurity Institute Journal.

These are exciting times in the cybersecurity community with news of ongoing cyber breaches, new legislation, and numerous meetings that seek to dissuade hackers from attacking our digital systems. Here at NCI, through our journal, we continue to increase awareness and knowledge of the cybersecurity discipline to help everyone better understand and meet the escalating challenges in the cyber community. In this latest issue, you will find seven informative articles from notable authors with a variety of perspectives on the field.

In our first article, Ping Wang presents us with “Project-based Curricular Service Learning for Cybersecurity Education,” a paper that proposes a project-based curricular service learning model to enhance education and career preparation in cybersecurity. Next, the team of Samrat Chatterjee, Ramakrishna Tipireddy, Matthew Oster, and Mahantesh Halappanavar provides us with their paper, “A Probabilistic Framework for Quantifying Mixed Uncertainties in Cyber Attacker Payoffs,” which highlights the importance of quantifying several sources and types of uncertainty impacting cyber attacker payoffs (defined as a penalty or reward based on actions) within a problem space. In his offering, Chris Golden suggests that “Creating New Private-Public Partnerships in Cybersecurity” can help create an environment that fosters cooperation between the private and public arenas and might create a larger incentive for businesses to join a cybersecurity partnership. Next, Debasis Bhattacharya and Debra A. Nakama discuss in detail the cybersecurity issues that relate to small businesses in their article, “Evolution of Information Security Issues in Small Businesses.” Aparicio Carranza and Casimer DeCusatis provide us with an interesting look at the flipped classroom in their offering, “Hybrid Implementation of Flipped Classroom Approach to Cybersecurity Education.” Malware is an ongoing issue, and Sean McVey presents an interesting look at it with “Malware Fingerprinting: Analysis of Tool Marks and Other Characteristics of Windows Malware.” Finally, we all recognize the importance of appropriate incidence response to a cyber attack and Austen Givens provides the reader with an in-depth look at it with “Strengthening Cyber Incident Response Capabilities Through Education and Training in the Incident Command System.”

The editors at NCI Journal believe these articles will continue to educate our readers and provide them with useful information that can be applied to their own systems and organizations to strengthen their systems cybersecurity.

The security of your digital system is of prime importance to you and your stakeholders, and we work continually to publish articles that you, our readers, will find helpful in your organization. Many thanks go to all the contributors, administration, and staff for their ongoing efforts to bring this latest edition of the National Cybersecurity Institute Journal to fruition. I look forward to your comments, suggestions, and future submissions to the journal.



Jane A. LeClair, EdD  
Editor in Chief



# Project-based Curricular Service Learning for Cybersecurity Education

Ping Wang

## ABSTRACT

Cybersecurity is a fast-growing career field with increasing challenges for educators. Service learning can be an effective educational method to improve career knowledge, skills, and professionalism. This paper proposes a project-based curricular service learning model to enhance education and career preparation in cybersecurity. The model proposes that student experience, discovery, and learning from course-related service projects are key elements to improving readiness for the cybersecurity profession. The proposition is supported by data and findings from a longitudinal study using a service learning project and team collaboration.

## INTRODUCTION

Cybersecurity, traditionally known as information security, is a fast-growing career field due to soaring and costly cyber crimes. College programs in cybersecurity typically prepare graduates for entry-level positions, such as cybersecurity analysts. According to the United States Department of Labor Bureau of Labor Statistics (BLS), employment of information security analysts is projected to grow 37% from 2012 to 2022, much faster than the average growth rates of 11% for all occupations and 18% for all computer-related occupations (United States Department of Labor, 2014). There is a national shortage of cybersecurity professionals with the right knowledge and skills, and education is expected to be the key solution

(RAND National Security Research Division, 2014). Therefore, there are increasing demands and opportunities for cybersecurity education and training.

Meanwhile, serious challenges exist for cybersecurity education. Cybersecurity is a new area based on the traditional computing profession and requires students to have a strong background and preparation in computer and information science and technology to succeed academically and professionally. However, there has been a perpetuated failure of education in the United States to prepare a strong and world-leading workforce in computing professions (Patterson, 2005). Major characteristics of this failure in U.S. undergraduate computing programs include outdated curricula, declining enrollment, and ignoring service learning opportunities that build application skills (Morelli, de Lanerolle, & Tucker, 2012). The outdated curricula and course content and lack of knowledge application experience may be the leading cause for the gap between the students' learning and the actual skills needed in the employment market. A recent graduate in computer software engineering from a major public university gives a vivid description of such a gap after his failure to find a job despite the fact that he graduated at the top of his engineering class: My college education left me totally unprepared to enter the real workforce. My degree was supposed to make me qualified as a programmer, but by the time I left school, all of the software and programming languages I'd learned had been obsolete for years (Ark, 2014, para. 3).

To address the cybersecurity needs and coordinate the national effort on improving cybersecurity education, training, and professional development, the U.S. National Initiative for Cybersecurity Education (NICE) was established. The mission of NICE is "to enhance the overall cybersecurity posture of the United States by accelerating the availability of educational and training resources designed to improve the

cyber behavior, skill, and knowledge of every segment of the population—enabling a safer cyberspace for all” (National Initiative for Cybersecurity Careers and Studies, US Department of Homeland Security, n.d., para. 2). This mission underscores the importance of both knowledge acquisition and knowledge sharing in the communities of our society for the benefit of everyone’s security in the cyberspace.

To help bridge the gap between college education offering and the job skills needed in the real world, this paper proposes a project-based curricular service learning model for cybersecurity education. The service learning model provides constructive and valuable opportunities for students to actively apply their learning to real world situations, gain authentic hands-on experience, improve their skills in collaboration, reflection and critical thinking, and cultivate strong professional and community service ethics that are critical to a successful career. This paper also reports and discusses the empirical data and findings in support of the model.

## CONSTRUCTIVE SERVICE LEARNING: THEORIES AND MODELS

Solid career preparation requires constructive student-centered learning and growth through education. Service learning is both a practical service and a constructive learning process that involves active knowledge inquiry, discovery, and acquisition and sharing. Bruner (1961) defines discovery learning as all forms of knowledge acquisition by using one’s own mind such as those used in curricula projects. Curricula service learning is guided by and complements class instruction. A curricula service learning project is an enhanced discovery learning process assisted by the instructions, guidelines, examples, and feedback from the course instructor rather than a totally independent self-inquiry by a student. Research indicates that enhanced discovery learning is much more effective than unassisted discovery or independent inquiry (Alfieri, Brooks, & Alderich, 2011). This type of discovery learning is often referred to as constructivism, which emphasizes the active role of the learner in knowledge acquisition and application.

Comprehensive analysis of 11 service learning research studies involving over 2,000 undergraduate students suggests that service learning has had statistically significant and positive effects on student learning outcomes (Warren, 2012). In cybersecurity workforce preparation, human capital and cybersecurity knowledge are the essential factors for achieving technical competence in the general cybersecurity competency model (United States Government Accountability Office, 2011). Knowledge is the contextual and high-value form of information and experience ready to apply to decisions and actions (Davenport, De Long, & Beers, 1998). Knowledge consists of both explicit knowledge or communicable information and tacit knowledge, which is personal and intuitive insight and know-how originated from individual experiences and values (Desouza, 2003). Service learning provides such individual experiences for acquiring and sharing explicit and tacit knowledge. In addition, the theory of reasoned action states that individual perception and attitude are a determining factor of one’s behavioral intention that predicts one’s actual behavior (Fishbein & Ajzen, 1975). Prior research results indicate a significant positive correlation between individuals’ cybersecurity knowledge and their intention and attitude toward cybersecurity technology (Wang, 2010, 2013). This paper proposes that service learning experience positively contributes to students’ motivation and success in learning. In other words, students’ service learning experience and knowledge acquisition in cybersecurity improve their perceptions and attitude toward cybersecurity technology, which in turn improves their motivation for learning behavior and success in cybersecurity education.

Service learning brings many positive pedagogical effects that enhance learning, and the most significant gains are in application experience, critical thinking through reflection, professionalism and community service ethics, and attitude and motivation for learning. Through hands-on learning-by-doing service learning activities, such as community service projects, internships, practica, and research projects, students make significant gains in their knowledge and skills (such as security awareness) and in their ability to contribute to the welfare of their communities (Aldas, Crispo, Johnson, & Price, 2010; Lincke, 2011). Service learning is a process that involves frequent reflection on knowledge and experience that enhances critical



thinking and learning. Reflection is a critical thinking activity that demonstrates one’s abilities and skills in connecting experience, observation, theories, reasoning, and learning objectives. In service learning, reflection activities, such as written or oral reports and presentations, encourage and enable students to explore, discover, and evaluate relationships between the course content learned from readings, lectures, and discussions, and their real experiences from doing the service learning work for the community (Ahmed, Hutter, & Plaut, 2008).

Service learning also contributes to the development of students’ professional and community service ethics. Through service learning experience, students learn to serve the community with pride and ethical behavior, increase their recognition of civic responsibilities and social justice, and develop a life-long habit of community service and civic involvement (Aldas, Crispo, Johnson, & Price, 2010; Meaney, Griffin, & Bohler, 2009; Steinberg, Bringle, & Williams, 2010). Students’ successful service learning project experience could lead to a higher perceived usefulness of the course content and materials and better attitude and intention to accept and use the course materials (Evangelopoulos, Sidorova, & Riolli, 2003). Prior research also indicates that service learning that integrates academic content and community service improves students’ academic interest and their attitude and motivation for learning, which leads to improved student engagement and retention (Morelli, de Lanerolle, & Tucker, 2012; Simonet, 2008).

Service learning also contributes to the development of students’ professional and community service ethics. Through service learning experience, students learn to serve the community with pride and ethical behavior, increase their recognition of civic responsibilities and social justice, and develop a life-long habit of community service and civic involvement (Aldas, Crispo, Johnson, & Price, 2010; Meaney, Griffin, & Bohler, 2009; Steinberg, Bringle, & Williams, 2010). Students’ successful service learning project experience could lead to a higher perceived usefulness of the course content and materials and better attitude and intention to accept and use the course materials (Evangelopoulos, Sidorova, & Riolli, 2003). Prior research also indicates that service learning that integrates academic content and community service improves students’ academic interest and their attitude and motivation for learning, which leads to improved student engagement and retention (Morelli, de Lanerolle, & Tucker, 2012; Simonet, 2008).

Service learning may occur in various forms based on different models. Heffernan (2001) identifies and describes six models for service learning. Table 1 below summarizes the six models, the student role, and the stated benefit for each model. These models primarily reflect the types of service learning activities and emphasize the perspective of the curricular design while ignoring the specific knowledge and skill objectives for student learning. The models are generic and not specifically designed for a certain discipline.

TABLE 1: HEFFERNAN’S SERVICE LEARNING (SL) MODELS

MODEL	STUDENT ROLE	BENEFIT
DISCIPLINE-BASED SL MODEL	Regular presence in the community and reflection on course content	Improve understanding of theoretical concepts
PROBLEM-BASED SL MODEL	Serve as “consultants” on specific community problem or need	Alleviate logistic difficulties for regular weekly commitments
CAPSTONE COURSE MODEL	Apply previous course work to relevant service work in the community	Help students transition from theory to practice
SERVICE INTERNSHIP MODEL	Work 10–20 hours a week in the community with faculty guidance	Develop skills while seeing contribution to the community
COMMUNITY-BASED ACTION RESEARCH MODEL	Work with faculty to learn research methods while serving as advocate for the community	Most effective for small classes and groups of students
DIRECTED STUDY ADDITIONAL/ EXTRA CREDIT MODEL	Work with an instructor to complete additional work or more in-depth work on a subject for additional credit	Good choice for self-directed and motivated students

TABLE 2: NEJMEH'S THREE-DIMENSIONAL SERVICE-LEARNING MODEL

PROJECT TYPE	ACTIVITY RANGE	PROJECT MODE
<b>TRAINING</b> <i>(share knowledge or skills)</i>	Research <i>(problem identification and concept definition)</i>	Cocurricular <i>(community service completed outside classroom; either university-based or non-university-based)</i>
<b>PROFESSIONAL SERVICES</b> <i>(provide expert advice)</i>	Analysis <i>(requirements discovery, documentation, process/system validation)</i>	Curricular <i>(project completed in the context of a college course – common project course, subdiscipline-specific project course, or an interdisciplinary course)</i>
<b>SYSTEM SELECTION</b> <i>(identify system needs and recommend solutions)</i>	Design <i>(architecture and design of database, user interface, communications, workflow, report, and solution strategy)</i>	Hybrid <i>(cooperative style of completing a project involving both a cocurricular component and a curricular or course-based component)</i>
<b>SUPPORT/HELP DESK</b> <i>(provide customer support)</i>	Implementation <i>(system implementation with details)</i>	
<b>CUSTOM DEVELOPMENT</b> <i>(develop custom applications)</i>	Test <i>(system integration, testing user acceptance, and validation of solution effectiveness)</i>	
<b>PRODUCT DEVELOPMENT</b> <i>(develop common product applications)</i>	Transition <i>(system installation and migration and delivery of tested system)</i>	
	Assessment <i>(assessing system or service performance, efficiency, effectiveness, and value/impact)</i>	

Nejmeh (2012) offers a more fine-grained three-dimensional model, which includes project types, activity range, and project mode for service learning. Compared with Heffernan's models, Nejmeh's three-dimensional model provides more specific categories of service learning activities with expected focus and skills. It is also practically more relevant to service learning in computing and cybersecurity education as the descriptions and examples are specifically based on computer and information science disciplines and sub-disciplines. Table 2 summarizes the three dimensions of this model.

## METHODOLOGY

The study in this paper is based on a planned longitudinal study using a community-based service learning project assignment required for an undergraduate credit course in cybersecurity conducted at a large urban public non-profit college in northeast U.S. with both online and on-site deliveries. The study period is three and a half years from the Fall 2011 semester to the Fall 2014 semester. The service learning project assignment is weighted as 10% in the student overall

course grade. During the last three semesters of the research (in spring, summer, and fall of 2014), the team work option is added to the project to evaluate student collaboration in service learning. The project design for the study includes the following topics related to the course content: training/tutoring (sharing cybersecurity knowledge and/or skills), professional services (providing expert advice on a cybersecurity issue related to the course content), system selection (identifying cybersecurity needs and recommending solutions), and support/help desk (providing technical support and troubleshooting on cybersecurity topics). The expected activities involved in the service learning project include research, analysis, testing, transition (installation), and assessment of cybersecurity issues and solutions. The project deliverable is a written report from the student summarizing the project experience, activities performed, person(s) worked with, accomplishments, and reflections on lessons learned and areas for improvement.

The project mode is curricular because it is primarily based on the cybersecurity knowledge, concepts, and skills in the course content. The project is an enhanced or assisted discovery learning process as necessary guidance and feedback are given in class. Though in

curricular mode, the project gives students abundant freedom to discover and pursue their specific topics of interest. Students' project reports are evaluated with feedback from the instructor. The total number of participants in the service learning project is 296 registered students from 11 sections of the course in 3.5-year research period. The following section presents the data, findings, and discussions from the study.

## FINDINGS AND DISCUSSIONS

The total number of participants in the service learning project is 296 registered students from 11 sections of the course in 3.5-year research period. Table 3 summarizes the data on the project type and activity range of the service learning reports submitted by the students. The Category column shows the

specific project type and the activity range of student submissions. The Total column shows the total count of each category. The Percentage column shows the percentage of each category relative to the total subject population (296).

The data in Table 3 shows a variety of project types and a wide range of activities, which involve heavy hands-on experience of applying the knowledge and skills from the course to real world situations in the community. The project types include training/tutoring, professional service, recommendation on system selection, and technical support and troubleshooting on various cybersecurity topics covered in the course. The service activity range includes research, analysis, system testing, system installation, and performance assessment. The three-semester team work data shows that nearly half of the students voluntarily participated in team work, which is an

TABLE 3: SUMMARY OF DATA ON PROJECT TYPE, ACTIVITY RANGE, AND TEAM WORK

	CATEGORY	TOTAL	PERCENTAGE
PROJECT TYPE	Training/tutoring ( <i>sharing cybersecurity knowledge and/or skills, such as on various cybersecurity risks</i> )	194	65.54%
	Professional services ( <i>providing expert advice on a cybersecurity issue related to the course content</i> )	21	7.09%
	System selection ( <i>identifying cybersecurity needs and recommending solutions</i> )	18	6.08%
	Support ( <i>providing technical support and troubleshooting on cybersecurity topics</i> )	63	21.28%
ACTIVITY RANGE	Research ( <i>problem identification and concept definition</i> )	65	21.96%
	Analysis ( <i>requirements discovery, documentation, process/system validation</i> )	82	27.70%
	Test ( <i>system integration, testing user acceptance, and validation of solution effectiveness</i> )	55	18.58%
	Transition ( <i>system installation and migration and delivery of tested system</i> )	51	17.22%
	Assessment ( <i>assessing system or service performance, efficiency, effectiveness, and value/impact</i> )	43	14.53%
TEAM WORK	A team of two collaborates on a service learning project with individual reports submitted; team work is optional.	37	46.83%

indicator of substantial interest in collaboration with others. Students performing the training or service as well as the trainees and recipients of the student service have reported remarkable experiences of knowledge discovery on important cybersecurity concepts. Additionally, students reported progress and achievement in conducting hands-on activities on important cybersecurity issues, such as cybersecurity and privacy research, and the selection, installation, configuration, and assessment of anti-virus and firewall protection solutions and products to secure valuable personal computers and data.

The hands-on application experience from the service learning has contributed significantly to students' success and enjoyment in learning. Over 90% of the student participants in the service learning project have reported a positive, enjoyable, and worthwhile experience of using their knowledge and skills, sharing their knowledge with the community, and discovering and learning something new on the cybersecurity topics for their project. The longitudinal assessment results also support students' improvement in learning through the service learning project. The course success rate among the student participants of the service learning project in the 3.5-year study period is over 91%, which is 13% higher than the average success rate among the students in this course without the service learning project during the previous three years. The course success rate among the team work participants is over 96% among the three semesters in 2014 with the team work option.

The service learning project experience has also developed students' reflection habit and critical thinking skills, which are essential to their success in learning. Critical reflection is a fundamental component of all service learning experiences and pedagogy, which is especially important for STEM disciplines to assess and critique the community's technology needs and the impact of service learning projects (George, 2012). All the reports submitted for the service learning projects include a section of reflection and comments on the experience. For example, many students were surprised that the people they worked with had no idea about basic computer protection knowledge and skills. Most students have also reported that they realized that

they need to learn more about a certain topic to do better on the service, such as analyzing computer data communications using a network analyzer.

The service learning project has also developed and improved students' professionalism and community service ethics. Professional and ethical behavior is especially important for information systems professionals as sensitive systems and information are often at stake (Hilton & Mowry, 2012). Professional and ethical behavior with a strong sense of responsibility and care for the well-being of others in the community is even more important for information systems security issues. Students have reported discovery of the importance of legal and ethical rules and guidelines for cybersecurity professionals, such as HIPPA for dealing with private health information in digital format. The majority of the students have reported great pleasure and pride in helping others in the community through the service learning project. The majority of the trainees and recipients of the service have reported positive behavior of the students, including being "responsible," "professional," "caring," "knowledgeable," "helpful," and "patient". The observation data is collected from the required confirmation letters signed by the recipients of the student service.

Another important reward for students in the service learning is the improvement in their attitude and motivation for learning, which will have a long-term positive effect on their future education and careers. The majority of the participating students have reported that the service learning project is such an enriching and rewarding learning experience that they found the cybersecurity course content very useful and interesting and would love to pursue further education and a future career in this field. The increased interest and motivation for learning may be attributed to the actual hands-on learning, service ethics, and reinforcement from the community as a result of the service learning experience.

## CONCLUSION

The project-based curricular service learning used in this 3.5-year study has improved students' overall academic success as well as their reflection and critical thinking, professional and community service ethics, and attitude and motivation for knowledge discovery and sharing. There are several areas for improvement in the future. First, given the initial success of the service learning project, more course work and weight in grading could be devoted to service learning to maximize students' learning through service. Also, a solution is needed to facilitate increased team work and collaboration in the service learning projects among online students who are geographically scattered. Students working together on service learning team projects need frequent physical presence together and communication. A potential solution is to design virtual service learning projects where students could perform service components individually in distributed locations while collaborating and communicating online in research, analysis, discussions, and assessment. In addition, it would be desirable to develop stable partnerships with community and industry organizations who can provide more frequent and regular opportunities for students to perform service learning projects.

## REFERENCES CITED

- Ahmed, Z., Hutter, L., & Plaut, J. (2008). Reflection in Higher Education Service-Learning. Scotts Valley, CA: Learn and Serve America's National Service-Learning Clearinghouse.
- Aldas, T., Crispo, V., Johnson, N., & Price, T. A. (2010). Learning by doing: The Wagner plan from classroom to career. *Peer Review*, 12 (4). Retrieved from <http://www.aacu.org/peerreview/pr-fa10/Aldas.cfm>
- Alfieri, L., Brooks, P. J., & Alderich, N. J. (2011). Does discovery-based instruction enhance learning? *Journal of Educational Psychology*, vol. 103 (1), 1-18.
- Ark, C. (2014, August 27). I studied business and programming, not English. I still can't find a job. *The Washington Post*. Retrieved from <http://www.washingtonpost.com/posteverything/wp/2014/08/27/i-studied-engineering-not-english-i-still-cant-find-a-job/>
- Bruner, J. S. (1961). The act of discovery. *Harvard Educational Review*, vol. 31, 21-32.
- Davenport, T. H., De Long, D., & Beers, M. (1998). Successful knowledge management. *Sloan Management Review*, vol. 39, 43-57.
- Desouza, K. (2003). Facilitating tacit knowledge exchange. *Communications of the ACM*, vol. 46, June 2003, 85-89.
- Evangelopoulos, N., Sidorova, A., & Riolli, L. (2003). Can service-learning help students appreciate an unpopular course? A Theoretical Framework. *Michigan Journal of Community Service Learning*, Winter 2003, 15-24.
- Fishbein, M., & Ajzen, I. (1975). Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. Reading, MA: Addison-Wesley.
- George, C. (2012). Is the community partner satisfied? In B. A. Nejmeh (Ed), *Service-learning in the computer and information sciences* (pp.517-530). Hoboken, NJ: John Wiley & Sons, Inc.
- Heffernan, K. (2001). Fundamentals of Service-Learning Course Construction. RI: Campus Compact, 2001, pp 2-9.
- Hilton, T. S. E., & Mowry, D. D. (2012). Teaching information systems ethics through service-learning. In B. A. Nejmeh (Ed), *Service-learning in the computer and information sciences* (pp. 243-257). Hoboken, NJ: John Wiley & Sons, Inc.
- Lincke, S. J. (2011). Service learning in security. *Proceedings of the 15th Colloquium for Information Systems Security Education, Fairborn, Ohio, June 13-15, 2011*, 63-68.
- Meaney, K., Griffin, K., & Bohler, H. (2009). Service-learning: A venue for enhancing pre-service educators' knowledge base for teaching. *International Journal for the Scholarship of Teaching and Learning*, 3 (2), 1-17.
- Morelli, R., de Lanerolle, T. R., & Tucker, A. (2012). The humanitarian free and open-source software project: Engaging students in service-learning through building software. In B. A. Nejmeh (Ed), *Service-learning in the computer and information sciences* (pp.117-136). Hoboken, NJ: John Wiley & Sons, Inc.
- National Initiative for Cybersecurity Careers and Studies, US Department of Homeland Security. (n.d.). Retrieved from <http://niccs.us-cert.gov/header/niccs-helping-you-enhance-your-cybersecurity-knowledge>
- Nejmeh, B. A. (2012). A framework for service-learning in the computer and information sciences. In B. A. Nejmeh (Ed), *Service-learning in the computer and information sciences* (pp.117-136). Hoboken, NJ: John Wiley & Sons, Inc.
- Patterson, D. (November, 2005). Rescuing our families, our neighbors, and ourselves. *Communications of the ACM*, 48 (11), 29-31.
- RAND National Security Research Division. (2014). *Hackers wanted: An examination of the information security labor market*. Retrieved from [http://www.rand.org/content/dam/rand/pubs/research\\_reports/RR400/RR430/RAND\\_RR430.pdf](http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf)
- Simonet, D. (2008). Service-learning and academic success: The links to retention research. *Minnesota Campus Compact*, May 2008, 1-13.
- Steinberg, K. S., Bringle, R. G., & Williams, M. J. (2010). Service-learning research primer. Scotts Valley, CA: National Service-Learning Clearinghouse.
- United States Department of Labor. (2014). Retrieved from <http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6>
- United States Government Accountability Office (GAO). (2011). *Cybersecurity human capital*. Retrieved from <http://www.gao.gov/products/GAO-12-8>

Wang, P. (2013). Assessment of Cybersecurity knowledge and behavior: An anti-phishing scenario. *Proceedings of ICIMP 2013: The Eighth International Conference on Internet Monitoring and Protection, Rome, Italy, June 23-28, 2013*, 1-10.

Wang, P. (2010). Information security knowledge and behavior: An adapted model of technology acceptance. *2nd International Conference on Educational Technology and Computer (ICETC), June 2010*, 364-367. DOI: 10.1109/ICETC.2010.5529366.

Warren, J. L. (2012). Does Service-Learning increase student learning?: A meta-analysis. *Michigan Journal of Community Service Learning*, Spring 2012, 56-61.

---

## AUTHOR

---

**Ping Wang** ([pwang2050@yahoo.com](mailto:pwang2050@yahoo.com)) is a professor of cybersecurity at the Graduate School of University of Maryland University College, where he teaches courses in cybersecurity, network security, pen testing, and digital forensics and also served as director of the master's program in cybersecurity for two years. Dr. Wang holds a master's degree in computer information science and a doctorate in information systems with specialization in e-commerce security risks and decisions. Dr. Wang is a Certified Information Systems Security Professional (CISSP) with consulting and development experience in cybersecurity and information systems and technology.

# A Probabilistic Framework for Quantifying Mixed Uncertainties in Cyber Attacker Payoffs

Samrat Chatterjee | Ramakrishna Tipireddy | Matthew Oster | Mahantesh Halappanavar

## ABSTRACT

Recent cybersecurity incidents involving data theft from the U.S. Office of Personnel Management have heightened the importance of designing *resilient* cyber systems that can support mission goals when compromised. However, securing such systems on a continual basis against multiple types of malicious attacks is an ongoing challenge. Cyber system administrators (defenders) typically have limited protective resources that need to be effectively allocated to thwart cyber attackers operating at relatively low costs. Game theory-based mathematical modeling approaches (involving strategic decision-makers) are increasingly being adopted for such cybersecurity challenges. This paper contributes to the state-of-the-art by highlighting the importance of quantifying several sources and types of uncertainty impacting cyber attacker payoffs (defined as a penalty or reward based on actions) within this problem space. These uncertainties arise due to randomness or lack of knowledge associated with cyber system operational behaviors, attacker types, and attack and defense actions over time. This paper explores the mathematical treatment of such mixed payoff uncertainties. A probabilistic modeling framework for representing cyber attacker payoffs under uncertainty is presented and a conditional probabilistic reasoning approach is adopted to organize the dependencies between a cyber system's state, attacker type, player actions, and state transitions. This also enables the application of probabilistic

theories to propagate various uncertainties in the attacker payoffs. An additional goal of this paper is to increase awareness about this problem domain among practitioners and researchers, and encourage further advancements in this area.

## INTRODUCTION

Recent cybersecurity incidents involving data theft that impacted federal government employees and contractors (U.S. Office of Personnel Management, 2015) have heightened the importance of designing and maintaining sound cyber defense mechanisms that include proactive, preventative, and reactive cybersecurity measures. Securing cyber systems on a continual basis against multiple types of malicious attacks (e.g. confidential data theft, unauthorized web server access, or denial-of-service) is a challenging problem both from a research standpoint and in practice. Cyber system administrators (defenders) typically have limited available resources to allocate among a variety of protective measures. Cyber attackers, however, operate at relatively low costs. Thus, developing a *resilient* cyber system that can support mission goals when compromised is an important problem and is the topic of discussion within this paper.

To effectively allocate protective resources against multiple (often unknown) attackers, a cyber defender must account for uncertainties in attack types and cyber system operational behaviors over time. Mathematical modeling and analysis might provide a mechanism for structuring this resource allocation decision-making process. In particular, game-theoretic approaches involving strategic decision-makers (i.e. cyber attackers and defenders) with differing

objectives have been researched extensively over the past decade (Roy et al., 2010; Liang and Xiao, 2013). Prior studies indicate that further research should include enhanced focus on characterizing attacker payoff (defined as a penalty or reward received by a player based on actions within a game-theoretic setting) functions. Attacker penalty refers to the attack planning and execution costs. Attacker reward may be represented as the damage and disruption that follows a successful attack. These cyber attacker payoff functions are typically subject to uncertainties (due to randomness and lack of knowledge) associated with system operational states, attacker types, player actions, and state transitions.

This paper focuses on the development of a probabilistic modeling framework for representing cyber attacker payoffs under uncertainty. Various sources of payoff uncertainty include: (1) cyber system state, (2) attacker type, (3) choice of player actions, and (4) cyber system state transitions over time. A conditional probabilistic reasoning approach is adopted to organize the dependencies between a cyber system's state, attacker type, player actions, and state transitions. This also enables the application of probabilistic theories to propagate various uncertainties in the attacker payoffs. The paper aims to highlight this important uncertainty quantification problem space to the cybersecurity research community and discusses classes of stochastic games for cybersecurity, sources and types of attacker payoff uncertainties, and approaches for representation and propagation of these uncertainties within a probabilistic setting.

## STOCHASTIC GAMES FOR CYBERSECURITY

### Overview and Context

Game theory is a mathematical tool that aids decision-making between multiple entities acting in a system towards individual perceived outcomes. A game consists of two or more entities (or players), each equipped with a set of actions. Play of the game involves players choosing actions in some order resulting in a change in system state. Players assign values to such states; this value function is the primary decision driver within the game. Games are typically differentiated by how many players are involved, the order and length of play, whether the players cooperate or

compete against one another, and by how much information each player possesses of past play as well as of each other's system state values.

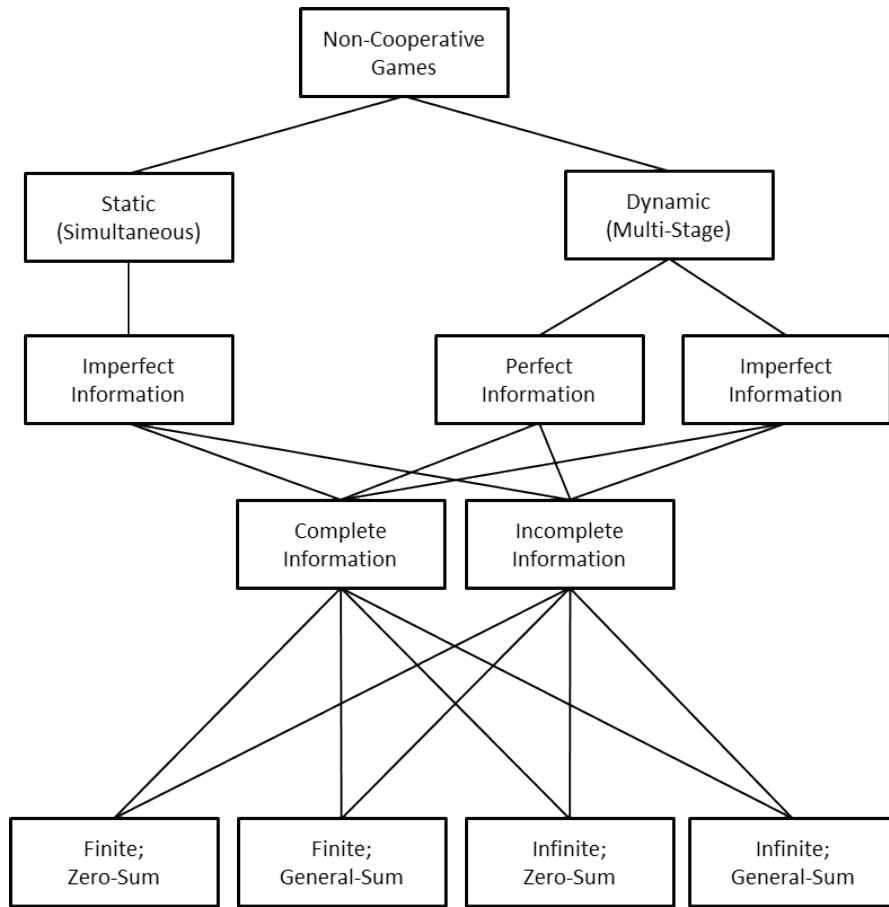
A simple example of a game is the well-known Prisoner's Dilemma (*Stanford Encyclopedia of Philosophy*, 2014). This game involves two players, both of whom are being questioned separately by authorities who believe at least one of the players has committed some crime. Either player may choose to cooperate with the authorities by confessing to the crime, or with each other by abstaining from talking to the interrogators. If both players talk, then they receive more time in prison than if they had both stayed silent. However, if only one player confesses, then he or she receives the largest prison sentence of any scenario, while the other (silent) player is free of any sentence. Since time in prison is valued as a penalty, the goal of each player is to take the action at some point in time which he or she believes will result in serving the least amount of time in prison.

Once the structure of the game is known, players must make decisions as to how they maneuver within the game by choosing a strategy. For example, one player in the Prisoner's Dilemma game might choose to confess to the crime immediately, believing that the other player might do the same. Do these individuals make their plays in response to the other's actions or simultaneously? Do they know which play each other will make or is some uncertainty placed on their choices? A common way for players to choose a (robust) strategy is to find a type of equilibrium or a set of player strategies where each is a best response to the others. In other words, if everyone committed to their respective strategy, then no single player would benefit from deviating.

In the context of cybersecurity, game theory plays a key role in helping defenders of cyber systems limit the impact of adversarial events (Liang and Xiao, 2013). For example, a cyber system administrator familiar with the network architecture, valuation of information contained within firewalls, and the types of attackers that would be interested in such information may utilize the theory of games to weigh certain sequences of protective actions against hypothetical attackers and ultimately plan more strategically under resource constraints. Figure 1 presents classes of



FIGURE 1: TYPES OF NON-COOPERATIVE GAME MODELS FOR CYBERSECURITY (ADAPTED FROM ROY ET AL., 2010)



non-cooperative games depicted by choosing a path from the top-most level to the bottom. In the next section, we formally define these concepts.

### Concepts and Notation

A *game* is a tuple  $(P, \mathcal{A}, \mathcal{U})$ , where  $P$  is a set of *players*,  $\mathcal{A} = \{A_p : p \in P\}$  is the collection of each player's set of *actions*,  $A_p$ , and  $\mathcal{U} = \{u_p : p \in P\}$  is the collection of each player's utility or payoff function  $u_p : \times_p A_p \rightarrow \mathfrak{R}$ . Let us define  $n := |P|$  and  $m_p := |A_p|$  for each  $p \in P$ . If  $n$ ,  $\sum_p m_p$ , and the number of rounds of play are all finite, then we say the game is a *finite game*; otherwise it is an *infinite*

*game*. If each action set is continuous, we say the game is *continuous*, and if each such set is discrete, it is (implicitly) called a *discrete game*.

Players play the game by choosing actions, or *acting*, at specified points in time. If each player acts only once in the game, it is said to be a *static game*, otherwise multiple stages of actions makes the game *dynamic*. The game is *simultaneous* if players act at the same time, otherwise it is *sequential*. Each action tuple  $a = (a_p : p \in P) \in A$ , where  $A := \times_p A_p$  is called a *play* of the game and has a value, or *payoff*, of  $u_p(a)$  to player  $p \in P$ . If  $\sum_p u_p(a) = 0$  for each  $a \in A$ , the game is a *zero-sum game*, otherwise

it is called a *general-sum game*. If the action sets of all players are identical and the utility functions are independent of who played each action, then the game has *symmetric* payoffs, and otherwise they are *asymmetric*.

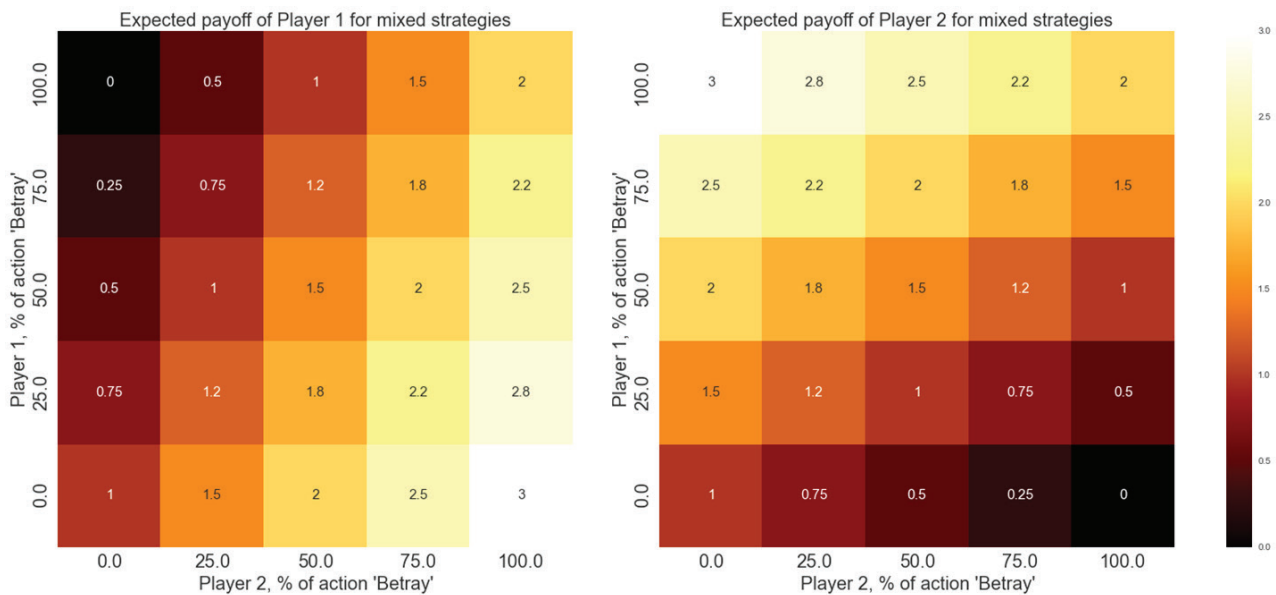
A *strategy set* for a player  $p \in P$  is the set  $X_p := \{x^p \in \mathbb{R}^{m_p} : \sum_{a_p} x_{a_p}^p = 1, x_{a_p}^p \geq 0 \forall a_p \in A_p\}$ , and each vector  $x^p \in X_p$  is called a *strategy*. A strategy  $x^p$  for any player is said to be *pure* if the support  $|\text{supp}(x^p)| = 1$ , and otherwise it is called a *mixed strategy* (i.e. if the play assigns some uncertainty to the actions to be taken). Given a tuple of player strategies  $x = (x^p : p \in P) \in X$ , where  $X := \times_p X_p$ , the *expected payoff* for player  $q \in P$  is the value of the function  $v_q(x) := \sum_{a \in A} u_q(a) * \prod_{p \in P} x_{a_p}^p$ .

Player  $p$  is deemed *rational* if decisions made at any point in time are always “best,” i.e. player  $p$  is considered rational if he or she chooses a strategy  $x^p \in X_p$  which maximizes his or her expected payoff  $v_p(x)$ , given some information about  $x^q$  for  $q \in P \setminus p$ ; otherwise, the player is *irrational*. In static and simultaneous games, a given tuple of strategies  $x \in X$  is called a *Nash equilibrium* if for each player

$p \in P$ , the value of  $v_p(x)$  is locally optimum, i.e.  $v_p(x) \geq v_p(y)$  for each  $y \in X$ , with  $y^q = x^q$  whenever  $q \neq p$ .

Figure 2 presents the concept of Nash Equilibrium pictorially using the Prisoner’s Dilemma example. Here we have two heatmaps, the left corresponding to the expected payoffs for Player 1 and the right to those of Player 2. We let the payoffs be quantified so that both players received two years in jail if both confess, one year in jail if neither confesses, and three years in jail for the single player betraying the other. Each plot’s y-axis represents the percentage of Player 1’s strategy dedicated to talking to authorities (“Betray”), while each x-axis represents the same but for Player 2’s strategy. The axes have been discretized and the values presented for any  $(x, y)$  strategy pair represent the corresponding player’s expected payoff. A Nash Equilibrium in this example is an  $(x, y)$  coordinate in which no cell within column  $y$  of the left plot is better (lighter in color) and similarly no cell within row  $x$  of the right plot is better (lighter in color). Thus, the bottom left corner  $(0,0)$  is a Nash Equilibrium, translating to a robust strategy for the players where neither should confess to the authorities.

FIGURE 2: PICTORIAL REPRESENTATION OF THE NASH EQUILIBRIUM CONCEPT



If every player is aware of every other player's payoff function and type, the game has *complete information*; otherwise it has *incomplete information*. Further, if every player knows all the past plays of the game, then the game has *perfect information* and otherwise *imperfect information*. A hierarchical diagram of these concepts is found in Figure 1. Notice that whenever a game is static, there can be no past information to learn, and hence all static games are, by default, imperfect games.

To relate these concepts back to our example, the Prisoner's Dilemma, we observed that the original interpretation of the problem is a finite, two-player, non-cooperative, static, simultaneous, general-sum game with imperfect and complete information and symmetric payoffs.

- It is considered a *finite* game since there are only two players, each with two distinct actions; if the players had infinitely many actions, e.g. degrees of involvement with distinct payoffs for each, or if play of the game continued on for an infinite number of rounds, then it would be classified as an *infinite* game.
- It is a *non-cooperative* game since the players cannot speak to one another (and we assume they have not planned their choices before being accused of the crime) and since they cannot form a coalition against another party; if communication were allowed then such a game would be a *cooperative* game.
- It is a *static* game, since each player gets one chance to confess before play is over; if the game had multiple stages (e.g., multiple crimes to confess to), then it would become *dynamic*.
- It is a *simultaneous* game, in essence, since neither player learns about the other's decision before play is over; if, however, once the first player confessed, the second one was notified before acting, this would change the game to *sequential*.
- It is a *general-sum* game since the sum of the payoffs over the players for any action is non-zero; if for every play one player lost in value what the other gained (e.g., monetary settlements), then this would become a *zero-sum* game.
- It is a game with *imperfect information* since there is no past; if, however, the players had been in this situation in the past for a different crime and the players' past decisions influenced present choices, then this would become a game with *perfect information*.
- It is a game with *complete information* since the players know each other's payoffs; if the players played according to an uncertain utility function of each play's payoff (e.g. one player gets paid to serve a longer sentence) which is further unknown to the opposing player, then we would have a game with *incomplete information*.
- Finally, the game has *symmetric* payoffs since each player receives the same sentence in similar scenarios; if, for example, one player had a previous record and would receive more time in jail upon confessing, then the game would become an *asymmetric* game.

To recap, we have the following high-level concepts categorized with some notation and key notes:

- **players** ( $p \in P, n: = |P|$ )
  - two or more decision-makers play the game
  - assume they act intelligently or *rationally*, i.e. never deviate from 'best'
- **actions** ( $A_p$  for  $p \in P$ )
  - player  $p$ 's *action* is an element  $a_p \in A_p$ , possibly *infinitely* many
  - a *play* is a tuple  $a: = (a_1, \dots, a_n)$  in the set  $A: = \times_p A_p$
- **payoff functions** ( $u_p(a)$  for  $a \in A$ )
  - each player  $p$  places a value  $u_p(a)$  on each play  $a \in A$
  - may not be reciprocal or *zero-sum*
- **information** ([in]complete, [im]perfect)
  - *complete* information means each player knows all others' payoff values for each play (know value of each possible outcome)
  - *perfect* means you know all previous plays (know history of plays and corresponding outcomes)

- play (sequential/simultaneous; static/dynamic)
  - *simultaneous* means no information on play before choosing one's own
  - *static* means only one act per player

## Game Implications for Cyber Systems

In cybersecurity, we typically model a non-cooperative game in which players act and where system state transitions reflect changes in the network's operational behavior. To this end, we augment the game tuple to include the finite—albeit generally very large—system state set  $S$ , and the transition function  $Q: S \times A \rightarrow S$  taking a state  $s \in S$  and a play  $a \in A$ , and transitioning it to the next state  $s' := Q(s, a)$ . The available actions for each player  $p \in P$  are limited to only those that make sense when the system is in the state  $S$  (e.g., a network administration will not shut down a file server when it is running normally, but he or she may do so when an adversary is observed stealing information from it); thus we distinguish these subsets with a superscript,  $A_p^S$ . Furthermore, any play  $a$  may probabilistically transition the state from  $S$  to many other states  $s'$ . We define this probabilistic function as  $T: S \times A \times S \rightarrow [0, 1]$ , and typically rewrite it as  $Pr(s'|s, a)$ , meaning  $T$  is the conditional probability function that yields the likelihood of sending the system from state  $s$  to  $s'$  whenever play  $a$  is made.

In the following section, various sources and types of uncertainties within game formulations are discussed. These uncertainties may arise from the system, player types/actions, and payoffs.

## UNCERTAINTIES IN CYBERSECURITY GAMES

### Modeling Preliminaries

In this paper, the probabilistic modeling framework for characterizing uncertain cyber attacker payoffs contains basic concepts from probability theory and utility theory. A few key concepts are briefly described below. Interested readers may refer to Ross (2004) or Clemen and Reilly (2001) for more detailed descriptions.

- **Random Variable:** A variable that can take different values (with probabilities) as a result of a random phenomenon. These variables may be *discrete* (expressed as probability mass functions) or *continuous* (expressed as probability density functions).
- **Marginal Probability:** The probability of occurrence of an event  $E_1$ ,  $Pr(E_1)$  that does not account for references, or depends on another event. For example, the probability of drawing a card with number 9 from a deck of cards is  $1/13$  (there are four 9's among 52 cards, so  $4/52 = 1/13$ ).
- **Conditional Probability:** The probability of occurrence of an event  $E_1$  given another event  $E_2$  occurs,  $Pr(E_1|E_2)$ . For example, the probability of drawing a card with diamond given that it has number 9 is  $1/4$  (there are four 9's and only one with diamond, so  $1/4$ ).
- **Joint Probability:** The probability of occurrence of events  $E_1$  and  $E_2$ ,  $Pr(E_1 \cap E_2)$ . For example, the probability of drawing a card with both a diamond and a number 9 is  $1/52$  (there are only one card with diamond and number 9 in a deck of cards, so  $1/52$ ).
- **Total Probability Theorem:** Let us assume  $n$  mutually exclusive events (events that cannot occur simultaneously)  $E_1, \dots, E_n$  with corresponding probabilities and  $\sum_{i=1}^n Pr(E_i) = 1$ ; then according to the Total Probability Theorem:  $Pr(A) = \sum_{i=1}^n Pr(A|E_i) \cdot Pr(E_i)$ , where  $A$  is an event of interest and  $Pr(A|E_i)$  is the conditional probability of event  $A$  given event  $E_i$  occurs.
- **Utility:** A concept from economics that is utilized as a measure of preference or satisfaction associated with a good or service. In the context of cybersecurity, it is associated with the payoffs that players receive within a game-theoretic setting.
- **Utility Function:** A mathematical function that depends on how a player values the realization of an operational state of the cyber system (in terms of dollars or time) and the probability of occurrence of that state. Utility functions may also be represented as probability distribution functions.

Let us now consider a game with an initial cyber system state  $s \in S$ , attacker type  $\alpha$  which depends on  $s$ , action tuple  $a = (a_1, a_2)$  of cyber system attacker and defender that depends on both  $s$  and  $\alpha$  and utility function (payoff) of player  $p$ ,  $u_p(s', a, \alpha, s)$  which is a function of the cyber system, attacker type, and player actions. Let us also assume that the system initially at state  $s \in S$  transitions to state  $s' \in S$  due to the action tuple  $a$  of the players (i.e., cyber system attacker and defender). The overarching objective is to quantify uncertainty in attacker payoff,  $u_{p_1}(s', a, \alpha, s)$  within a probabilistic modeling framework. In the context of cybersecurity, system state  $s$  may correspond to different operational conditions of the cyber network before, during, and after potential attacks. Some examples of cyber system states may include: “Normal\_operation”, “Httpd\_attacked”, “Website\_defaced”, and “Network\_shut\_down” (Lye and Wing, 2005). Attacker type  $\alpha$  refers to the capabilities in terms of skills and resources available to a cyber system attacker. Actions of the cyber system attacker and defender may or may not cause the system to transition from one state of operation to another. Examples of attacker actions may involve installing a sniffer, cracking a server access password, or capturing data whereas a defender may pursue actions including installing sniffer detectors, removing virus and compromised accounts, or restoring websites.

## Sources of Uncertainty

A non-cooperative cybersecurity game may involve the defender not having complete information about the system (due to partial observability) or the attacker (due to multiple attack possibilities at a point in time). These information gaps may include: (1) initial system state, (2) type of attacker, (3) combinations of attacker and defender actions, and (4) effects of these actions on system state transitions. We adopt a probabilistic framework to account for this lack of information and model these parameters as discrete or continuous random variables with appropriate uncertainty distributions. Expert judgment and/or available data from simulation experiments may be utilized to select the type of random variables and statistical methods to estimate these distributions and their parameters. Further, these uncertainties may be propagated to the quantities of interest (attacker payoff here) and its effect on the outcome of the game may be analyzed.

Our conceptual uncertainty model begins by assigning probability  $Pr(s)$  for initial system state  $s$  at the start of the game. Conditional probability  $Pr(\alpha|s)$  is used to define attacker type  $\alpha$  conditioned on initial system state  $s$ , since skills and resources required for an attack depend on initial system state. The action tuple  $a$ , depends on attacker type and system state — so we define probability of  $a$  as  $Pr(a|\alpha, s)$ . State transition probability from system state  $s$  to state  $s'$  is represented as  $Pr(s'|a, \alpha, s)$ . Payoff utility function of a player  $p$  depends on the initial system state, attacker type, action tuple, and new system state as  $Pr(u_p|s', a, \alpha, s)$ . In the following sections we describe methodologies for modeling these probabilities and propagating the uncertainty to player payoff utility  $u_p$  in terms of both marginal and conditional probabilities.

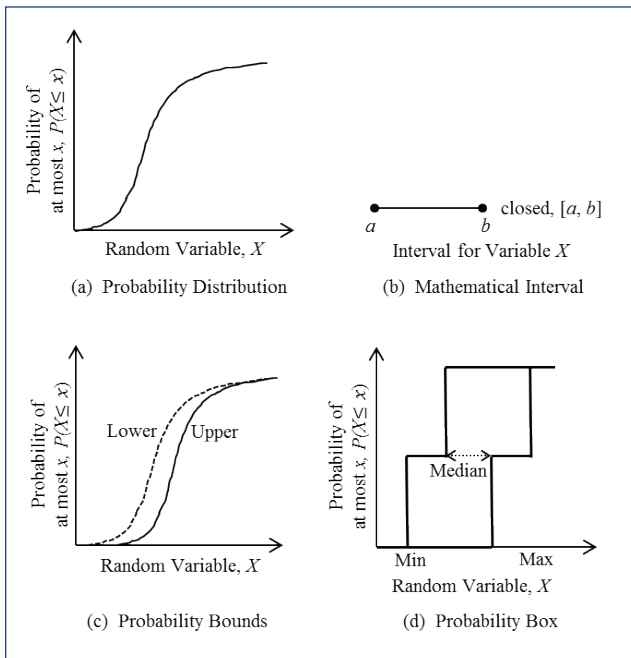
## Uncertainty Representations

A comprehensive modeling approach to securing a cyber system must account for the uncertain threats and system operational behaviors under time-varying conditions. Uncertainties in quantitative risk models arise from inherent randomness in samples (*aleatory*) or incomplete knowledge (*epistemic*) about fundamental phenomena (Pate-Cornell, 1996). A key distinction between these two types of uncertainty is that *epistemic* uncertainty can be reduced by gathering more information, whereas *aleatory* uncertainty is not reducible. These uncertainties may be present in the modeling elements/variables or the model itself. Thus, appropriate representation and propagation of uncertainty within these models is essential for distinguishing between the knowns and unknowns. In this paper, we describe the representation of uncertainties in input variables and discuss the propagation of these uncertainties to output variables of interest.

Uncertainty from randomness may be addressed through the use of statistical probability distributions, whereas incomplete knowledge may be represented using mathematical intervals (Abrahamsson, 2002). Figure 3 presents four uncertainty representations (probability distribution, mathematical interval, probability bounds, and probability box) for a hypothetical variable,  $X$ , with uncertain values. A probability distribution contains probabilities of occurrence of outcomes from a random experiment; mathematical interval is a set of real numbers between

lower and upper bounds; probability bound refers to a probability distribution with uncertain parameter values; and probability box represents limits of uncertain percentile values (e.g. median is the 50th percentile). The choice of uncertainty representation depends on data and knowledge associated with the variable of interest. Typically, probabilities may be defined using a frequentist approach (i.e. as an estimate of limiting relative frequency or ratio of the number of successful trials to total number of trials) or a Bayesian approach (i.e. as degree of belief with supporting information from statistical data, physical models, and subjective expert judgments).

FIGURE 3:  
UNCERTAINTY REPRESENTATIONS FOR  
HYPOTHETICAL VARIABLE,  $X$



### Uncertainty Propagation Methods

Methods for propagating uncertainty to the output variables within quantitative models depend on the representations associated with the uncertain input variables. Let us consider a thought experiment where  $\mathbf{x}$  represents a vector of  $k$  uncertain input variables; a single input variable is denoted as  $X$ ; and the model output  $y$  is a function of  $\mathbf{x}$ :  $y = g(\mathbf{x})$ . We outline below three mathematical approaches for uncertainty propagation based on probability distributions and

mathematical intervals. Please note that the list of approaches below is not exhaustive and represents initial methods identified by the authors for further investigation within a cybersecurity setting. For additional discussion, interested readers may refer to Abrahamsson (2002), Swiler et al. (2009), Walker et al. (2010), and Cox (2012).

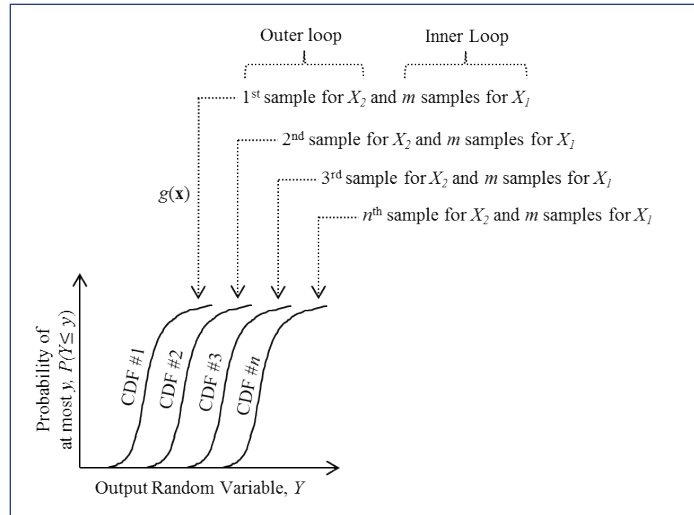
1. **Monte Carlo Sampling Analysis:** Let us assume an input random variable,  $X$  that has a cumulative distribution function  $F(X) = P(X \leq x)$  and an inverse cumulative distribution function  $F^{-1}(p) = x$ . If  $F(X)$  is strictly increasing and continuous, then  $F^{-1}(p)$ , where  $p \in [0,1]$ , is a real number  $x$  such that  $F(x) = p$ . To generate a random sample value for an input random variable,  $X$ , a random number,  $r$ , is first generated between 0 and 1 (there are several random sampling schemes available in the literature, including simple random sampling (where all samples have equal likelihood of being chosen) and Latin hypercube sampling (a stratified sampling scheme without replacement) (Abrahamsson, 2002)). This sampled value,  $r$ , is then passed through the inverse cumulative distribution function  $F^{-1}(r)$  to generate a random sample value,  $x$ . Similarly, random sample values for all  $k$  uncertain input variables may be generated resulting in a random sample vector,  $\mathbf{x}$ . The vector  $\mathbf{x}$  when passed through the function  $g(\mathbf{x})$  produces a random output value of  $y$ . This Monte Carlo sampling process may be repeated hundreds or thousands of times to generate a probability distribution for the output random variable  $Y$ .

2. **Interval Analysis:** This analysis allows the propagation of interval uncertainty to output variable,  $y$  when input variables,  $\mathbf{x}$ , are represented as intervals. The approach is computationally inexpensive, produces conservative uncertainty estimates, and is useful for conducting worst-case analysis. Let us assume two uncertain input variables  $X_1$  and  $X_2$ , represented as intervals  $[a, b]$  and  $[c, d]$  respectively. For basic arithmetic operations with:  $g(\mathbf{x})$  as  $X_1 + X_2$ ,  $y = [a + c, b + d]$ ;  $g(\mathbf{x})$  as  $X_1 - X_2$ ,  $y = [a - d, b - c]$ ;  $g(\mathbf{x})$  as  $X_1 \cdot X_2$ ,  $y = [\min(ac, ad, bc, bd), \max(ac, ad, bc, bd)]$ ; and  $g(\mathbf{x})$  as  $X_1/X_2$ ,  $y = [\min(\frac{a}{c}, \frac{a}{d}, \frac{b}{c}, \frac{b}{d}), \max(\frac{a}{c}, \frac{a}{d}, \frac{b}{c}, \frac{b}{d})]$  where 0 is not in  $[c, d]$ . These basic arithmetic properties may be extended further for evaluating more complex functions,  $g(\mathbf{x})$ .

3. **Two-phase Monte Carlo Sampling Analysis:** In certain applications, stochastic and knowledge-based forms of uncertainty in the input variables may be separated and analyzed further using a “two-phase” sampling approach. This approach involves two computational sampling loops: outer and inner. The outer loop contains input variables with knowledge-based uncertainty and the inner loop contains variables with stochastic uncertainty. A single iteration in the outer loop yields a sample (from the outer loop variables) that is passed to the inner loop, where several iterations involving samples from the inner loop variables are performed. Each sample combination of outer and inner loop variables when passed through a model results in a realization of the output variable of interest. Thus, several inner loop iterations result in an output variable distribution addressing stochastic uncertainty. Finally, multiple outer loop iterations lead to a collection of output variable distributions whose dispersion addresses knowledge-based uncertainty.

A graphical representation of this two-phase sampling analysis is in Figure 4. The sampling scheme may be based on multiple approaches, including random sampling or Latin hypercube sampling. For example, let us assume two uncertain input variables  $X_1$  and  $X_2$ , where  $X_1$  has a cumulative distribution function  $F(X_1)$  and  $X_2$  is represented as an interval  $[a, b]$ . Given a function  $g(\mathbf{x})$  as  $X_1 + X_2$ , the outer loop may comprise of realizations from  $X_2$  and the inner loop may contain realizations from  $X_1$ . Given a sample from the interval  $[a, b]$ , several samples (iterations) for  $X_1$  may be generated using its probability distribution via a Monte Carlo scheme. The vector  $\mathbf{x}$  (with several  $X_1$  sample values and the same  $X_2$  sample value) when passed through the function  $g(\mathbf{x})$  produces a probability distribution for the output random variable,  $Y$ . With multiple samples from the interval  $[a, b]$  and repetition of the sampling process above, a collection of output probability distributions are obtained. Each distribution for output random variable,  $Y$ , represents the stochastic uncertainty and the dispersion of distributions reflects the knowledge-based uncertainty.

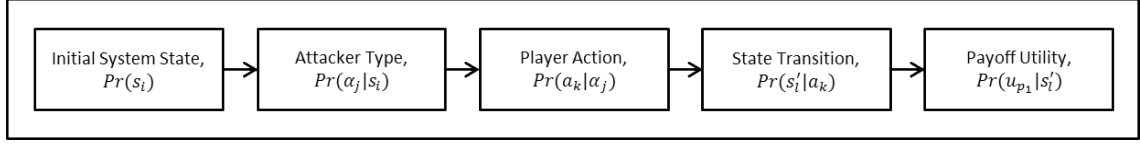
FIGURE 4:  
VISUAL REPRESENTATION OF TWO-PHASE MONTE CARLO SAMPLING ANALYSIS



## PROBABILISTIC FRAMEWORK FOR PAYOFF UNCERTAINTY QUANTIFICATION

The payoff uncertainty quantification framework presented here is an extension of the conceptual representation within prior work (Chatterjee et al., 2015) and is based on systems analysis, probability theory, and utility theory. Within this framework, uncertainty is modeled through marginal, joint, and conditional probability distributions associated with parameters of a stochastic cybersecurity game (see Figure 5). There are five elements within this modeling framework: (1) probability of initial cyber system state, (2) probability of attacker type, (3) probability of player action choices, (4) probability of cyber system state transitions over time, and (5) probability of attacker payoff utility. An underlying assumption here is that the cyber system is already compromised; as a result issues related to sensing during an attack is beyond the scope of this study. The probabilistic intuition within this framework initiates with the cyber system initially being in a particular state of operation. Multiple types of attacks may be launched to degrade system performance from that initial state. Based on system state conditions and attacker types, various player action choices may then be available. As a result of these player actions, the cyber system may or may not transition to other states of operation.

FIGURE 5: PAYOFF UNCERTAINTY QUANTIFICATION FRAMEWORK



(ADAPTED FROM CHATTERJEE ET AL., 2015)

Further, depending on the final state of operation, attacker payoff utilities may be assessed using probability distributions. This conditional probabilistic reasoning helps organize the dependencies among the system, attacker types, and player actions and enables the application of total probability theorem for payoff uncertainty propagation.

Mathematically, let  $Pr(s)$  be the probability of the system being in initial state  $s \in S$ , where  $S$  is a finite set of all possible system states. Let  $Pr(\alpha|s)$  be the probability of attacker type  $\alpha$  given initial system state  $s$ . Then  $Pr(a|\alpha, s)$  is the probability of players taking actions  $a$ , conditioned on the attacker type  $\alpha$  and the system state  $s$ . Let  $Pr(s'|a, \alpha, s)$  be the transition probability from system state  $s$  to state  $s'$  given action tuple  $a$  and attacker type  $\alpha$ . Let us also assume that these conditional and marginal distributions are available from domain experts or simulation experiments; the next step involves propagating these uncertainties into the attacker payoff utility and computing its probability distribution. The final outputs of interest are marginal and conditional probabilities of attacker payoff utility,  $Pr(u_{p_1})$ .

Using total probability theorem, the discrete version of the marginal attacker payoff probability is:

$$Pr(u_{p_1}) = \sum_i \sum_j \sum_k \sum_l Pr(u_{p_1}|s'_i, a_k, \alpha_j, s_i) \cdot Pr(s'_i|\alpha_k, \alpha_j, s_i) \cdot Pr(a_k|\alpha_j, s_i) \cdot Pr(\alpha_j|s_i) \cdot Pr(s_i)$$

In this case, all the dependent variables in the conditional distributions get integrated out. This quantity provides distributional information about overall attacker payoff utility, but does not reveal specific details such as the probability of attacker payoff utility with an assumed initial system state,  $s_i$  or against an assumed attacker type,  $\alpha_j$ . To reveal

these finer resolution details, we retain conditional probabilities, given specific quantities. For example,  $Pr(u_{p_1}|s_i)$ , is the probability of attacker payoff assuming an initial system state and is computed as:

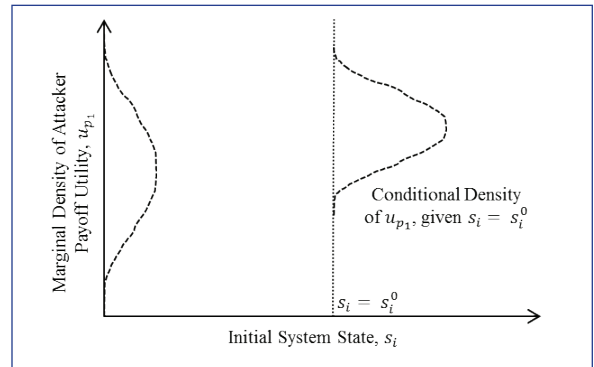
$$Pr(u_{p_1}|s_i) = \sum_j \sum_k \sum_l Pr(u_{p_1}|s'_i, a_k, \alpha_j, s_i) \cdot Pr(s'_i|\alpha_k, \alpha_j, s_i) \cdot Pr(a_k|\alpha_j, s_i) \cdot Pr(\alpha_j|s_i)$$

Similarly,  $Pr(u_{p_1}|\alpha_j, s_i)$  is the probability of attacker payoff given an assumed attacker type and initial system state and is computed as:

$$Pr(u_{p_1}|\alpha_j, s_i) = \sum_k \sum_l Pr(u_{p_1}|s'_i, a_k, \alpha_j, s_i) \cdot Pr(s'_i|\alpha_k, \alpha_j, s_i) \cdot Pr(a_k|\alpha_j, s_i)$$

Figure 6 presents notional attacker payoff marginal and conditional probability distributions. In this figure, marginal probability  $Pr(u_{p_1})$ , represents the overall uncertainty in attacker payoff. The conditional probability,  $Pr(u_{p_1}|s_i)$ , represents payoff uncertainty for an assumed initial system state. Different versions

FIGURE 6: NOTIONAL CYBER ATTACKER PAYOFF DISTRIBUTIONS





of attacker payoff probability distributions are essential inputs within cybersecurity game settings and are important for identifying optimal defender strategies needed for *resilient* design of cyber systems.

## CONCLUSION

Application of game theory-based mathematical modeling approaches (involving strategic decision-makers) for cybersecurity is a promising area of research inquiry. This paper contributes to the state-of-the-art by highlighting the importance of quantifying several sources and types of uncertainty impacting cyber attacker payoffs within this problem space. These uncertainties arise due to randomness or lack of knowledge associated with cyber system operational behaviors, attacker types, and attack and defense actions over time. Different classes of stochastic game models are discussed and approaches for representing and propagating uncertainty are identified. A conditional probabilistic reasoning approach is adopted to organize the dependencies between a cyber system's state, attacker type, player actions, and state transitions. A theoretical, probabilistic modeling framework for quantifying attacker payoff uncertainty is described and mathematical formulations of marginal and conditional probability distributions are presented. Implementation of our mathematical formulations in real-world systems may yield valuable payoff uncertainty inputs to large-scale cybersecurity games.

A detailed investigation of uncertainty quantification within cybersecurity games could lead to advances in proactive security resource allocation strategies for designing *resilient* cyber systems. A goal of this paper was also to increase awareness about this problem domain among practitioners and researchers, and encourage further advancements in this area.

## ACKNOWLEDGMENTS

This research study was supported by the Asymmetric Resilient Cybersecurity (ARC) initiative at the Pacific Northwest National Laboratory (PNNL). PNNL is a multi-program national laboratory operated by Battelle Memorial Institute for the U.S. Department of Energy under DE-AC06-76RLO 1830.

## REFERENCES CITED

- Abrahamsson, M. (2002). Uncertainty in quantitative risk analysis—characterization and methods of treatment. Report 1024, Department of Fire Safety Engineering, Lund University, Sweden, pp. 88.
- Chatterjee, S., Halappanavar, M., Tipireddy, R., Oster, M.R., and Saha, S. (2015). Quantifying mixed uncertainties in cyber attacker payoffs. *Proceedings of IEEE international symposium on technologies for homeland security (HST 2015)*, Waltham, Massachusetts, 1–6, doi:10.1109/THS.2015.7225287.
- Clemen, R.T., and Reilly T. (2001). *Making hard decisions with DecisionTools*, 2nd Edition. South-Western Cengage Learning, Mason, Ohio.
- Cox, L.A. (2012). Confronting deep uncertainties in risk analysis. *Risk Analysis*, 32(10), 1607–1629.
- Liang, X., and Xiao, Y. (2013). Game theory for network security. *IEEE Communications Surveys and Tutorials*, 15(1), 472–486.
- Lye, K.W., and Wing, J.M. (2005). Game strategies in network security. *International Journal of Information Security*, 4(1), 71–86.
- Paté-Cornell, M.E. (1996). Uncertainties in risk analysis: Six levels of treatment. *Reliability Engineering and System Safety*, 54, 95–111.
- Ross, S. (2004). *A first course in probability*, 6th Edition. Pearson Education, Delhi, India.
- Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., and Wu, Q. (2010). A survey of game theory as applied to network security. *Proceedings of 43rd Hawaii international conference on system sciences—IEEE Computer Society, Kauai, Hawaii*, 1–10, doi:10.1109/HICSS.2010.35.
- Stanford Encyclopedia of Philosophy. (2014). *Prisoner's Dilemma*. Center for the Study of Language and Information, Stanford University. Retrieved from <http://plato.stanford.edu/entries/prisoner-dilemma/>.
- Swiler, L.P., Paez, T.L., and Mayes, R.L. (2009). Epistemic uncertainty quantification tutorial. Proceedings of the *IMAC-XXVII: Conference & exposition on structural dynamics*, 1–17.
- U.S. Office of Personnel Management. (2015). Cybersecurity resource center. Retrieved from <https://www.opm.gov/cybersecurity>.
- Walker, W.E., Marchau, V.A.W.J., and Swanson, D. (2010). Addressing deep uncertainty using adaptive policies: Introduction to section 2. *Technological Forecasting and Social Change*, 77(6), 917–923.

## AUTHORS

---

**Samrat Chatterjee** ([samrat.chatterjee@pnnl.gov](mailto:samrat.chatterjee@pnnl.gov)) is an operations research scientist in the National Security Directorate at Pacific Northwest National Laboratory. His research focuses on assessing and managing risks to critical cyber and physical infrastructure systems from multiple hazards utilizing interdisciplinary modeling and simulation methods. He has published and presented over 30 contributions in refereed journals and conferences. Dr. Chatterjee conducted postdoctoral research on infrastructure risk and decision analysis at the U.S. Homeland Security National Center of Excellence for Risk and Economic Analysis of Terrorism Events (CREATE) at the University of Southern California and holds a doctorate in civil engineering with focus on systems risk analysis from Vanderbilt University.

**Ramakrishna Tipireddy** ([Ramakrishna.Tipireddy@pnnl.gov](mailto:Ramakrishna.Tipireddy@pnnl.gov)) is a postdoctoral research assistant in the Physical and Computational Sciences Directorate at the Pacific Northwest National Laboratory. His research interests include uncertainty quantification, computational mechanics, and development of reduced order models for complex stochastic systems. Dr. Tipireddy received his doctorate in civil engineering from University of Southern California.

**Matthew Oster** ([Matthew.Oster@pnnl.gov](mailto:Matthew.Oster@pnnl.gov)) is an operations research scientist with the National Security Directorate at Pacific Northwest National Laboratory (PNNL). His research areas and interests broadly include operational modeling and simulation, mathematical optimization algorithms, and decision support software development. Dr. Oster holds a doctorate in Operations Research from Rutgers, the State University of New Jersey, and a Bachelor of Science in mathematics.

**Mahantesh Halappanavar** ([hala@pnnl.gov](mailto:hala@pnnl.gov)) is a staff scientist in the Physical and Computational Sciences Directorate at the Pacific Northwest National Laboratory. His research interests include the interplay of algorithm design, architectural features, and input characteristics targeting massively multithreaded architectures such as the Cray XMT and emerging multicore and many-core platforms. Dr. Halappanavar received a doctorate in computer science from Old Dominion University.

# Creating New Private-Public Partnerships in Cybersecurity

Chris Golden

## ABSTRACT

Current efforts to produce partnerships between the public and private sectors in cybersecurity have met with little success. This is due to the fundamental mismatch between the interests of public and private sector actors. Better aligning these interests will help create an environment which fosters cooperation between the private and public arenas. In addition, changing the structure of government support to the business world might create a larger incentive for businesses to join a cybersecurity partnership. The combination of these two approaches, aligning interests and restructuring financial support could lead to a self-sustaining partnership where the interests of all parties are met while at the same time growing cybersecurity costs are controlled.

## INTRODUCTION

With the threats posed by malicious actors in cyberspace growing and evolving at an increasing rate, individuals, companies, and governments have a duty to take actions to mitigate these threats to our interconnected systems. The vulnerabilities are enormous, with almost all critical infrastructures in America and the communications nodes that connect them accessible via the Internet. The U.S. government is potentially not the primary target, but rather the critical infrastructure owned and operated by private companies which comprises over 70% (Treasury, 2013)

of the nation's critical infrastructure. Threat actors in cyberspace are targeting both private and public networks simultaneously. This is due to the fact that both business traffic and government traffic flow over the same commercially owned networks. Additionally, with government procurement buying many of the same systems, software, and other information technology appliances, the threat actors have no need to invest in breaking into two separate types of computer systems (Iasiello, 2012). Therefore, any response to critical infrastructure cybersecurity demands a coherent, disciplined and nation-wide effort.

Private companies do not have the resources or manpower to tackle this issue alone. The United States government must be willing and able to step in and provide assistance (Consortium, 2011). To date, efforts to form private-public partnership in the cybersecurity arena have made only modest gains. This is due to the basic variances in private and public sector interests. Private companies are driven by profit and look at cybersecurity costs in terms of the impact to the bottom line. Governments look at the potential consequences (Bures, 2013) of a lack of robust cybersecurity and want systems secured with much less concern for costs. These diverse interests are at the heart of current disagreements (Boardman & Vining, 2012) in private-public partnerships in cybersecurity. Governments want the private sector to pay for their own cybersecurity to a level that the government feels will successfully secure our critical infrastructure. They would also like for companies to report private information about the company's current security practices, network designs, and other data on potential or actual breaches of those systems. Not surprisingly, the private sector has little interest in either paying more for cybersecurity than they feel is necessary nor providing proprietary information to the government (Bures, 2013). They fear much of the proprietary information they report to the government will end up

in the hands of their competitors (Treasury, 2013). If not divulged in a government report, many companies fear this information would become accessible via a Freedom of Information Act request by their competitors. Many businesses view the current construct of private-public partnerships in cybersecurity as a one-way street. They fulfill their regulatory reporting requirements and yet no actionable information flows back to them from the government (Busch & Givens, 2013). The government highlights the sensitivity and classification (Treasury, 2013) of this information as to why there is little to no information flowing back to companies.

Any private-public partnership in cybersecurity must first address the differences in interests among all of the participants (Bures, 2013). A government assessment of the partnership will not sufficiently incentivize the private sector to join as principal participants in the process. Changes in both the structure of the partnership and in the incentives provided to those who the government wishes to participate must be successfully addressed for there to be real partnership development.

## SEPARATE INTERESTS

---

Understanding the differences in interests between the government on the one side and the private sector on the other when it comes to cybersecurity partnerships is the critical first step. Without addressing all of the participants' interests, there is little room to forge a new and better way forward for private-public partnerships in cybersecurity. Currently, there are very few similarities between these two groups of interests. Identifying the distinct differences in participants' interests is the first step toward creating a new model for cybersecurity partnerships.

Many of these differences originate from the two very distinct operating models the business and government communities utilize. The private sector focuses on profit-making and impacts to the bottom-line of their financial viability. They view costs, such as those necessary for a high level of cybersecurity, as something to be minimized. The higher costs of cybersecurity, especially to the level of cybersecurity their partners in the government would like them to achieve (Consortium, 2011), must come from somewhere and

it is the business's profit margin that takes the reduction. With the rise of litigation based on cybersecurity breaches (e.g. Sony, Target, etc.) and government approval of class action lawsuits, the tone emanating out of the C-suite in companies is slowly changing. To date, not enough change in these companies' operating models have occurred to justify a decrease in government interest in critical infrastructure cybersecurity.

The manner in which the business community addresses risk is also quite different from how the government addresses it. Risk is inherent in all business activities and therefore, experienced business professionals have learned to manage risk in multiple ways. These professionals have spent their entire business careers addressing and mitigating risks based on the risk's economic impact to the business. Mitigating risks in a resource constrained environment that will allow the business to remain afloat during a crisis and quickly recover their ability to generate revenue is at the heart of business risk mitigation strategies. If the perceived cost to the business of a cybersecurity protocol is more than the perceived cost of potential data loss or a breach of the company's networks, then many business professionals would opt to accept the risk versus expending funds for tighter cybersecurity. They are also conditioned to seek a return on investment for every dollar spent. Currently, there is little data to show the actual financial impact of cybersecurity strategies in real dollars for companies (Consortium, 2011). Presently, there are very few examples of real costs from potential breaches or data loss to compare to the up-front investment required to implement cybersecurity postures which might prevent these events from taking place. This leads many business professionals to accept their current level of risk since they cannot determine the right mix of cyber defenses.

The United States government, on the other hand, views security and risks under a completely different rubric. One of the primary duties of the government is to provide security for the population. It does this with much less regard for costs than within the corporate world. Obviously, the amount of resources available to the U.S. government for security is orders of magnitude more than the resources available to the private sector (Bissell, 2013). The U.S. government views the providing of security as one of the core functions driving its very existence. Threats

are assigned strategies and these strategies are then resourced accordingly and tracked to establish the success of failure of the strategy. It is little surprise that the government would apply the same basic principles to critical infrastructure cybersecurity. Therefore, the government expects private sector companies who own and operate our critical infrastructure to fully support not only the government's programs but also the government's views.

## INTERESTS ALIGNMENT AND RECOMMENDATION

Any future private-public partnerships in cybersecurity will need to adequately address both the interests of the U.S. government as well as the interests of the private sector to be successful. In the case today, too much focus is on the government's requirements and too little on the desires of the private sector. Therefore, there have been few notable achievements in these private-public partnerships. New programs will need to address all of the following interests:

- Private sector desires for:
  - Privacy or internal or proprietary information
  - Lower costs
  - Lower regulatory requirements
  - Other tools to assist in the management of cyber risks
- Governmental desires for:
  - Secure privately owned and operated critical infrastructure
  - Information from businesses on their cybersecurity programs and their results
  - Private sector participation in government cybersecurity programs

There is an example for a structure that would address a number of the interests above. It has not been applied to cybersecurity before but the legal and functional framework is already in place. The United States Air Force convenes two separate boards in event of an aircraft accident. One is an Accident Investigation Board (AIB) and the other is a Safety Investigation Board (SIB) (USAF, 2013). Typically,

the SIB convenes first and is completely focused on identifying the root cause of the accident in order to make any immediate changes to Air Force policies or guidance which might have led to the accident. This is done to ensure that the weapon systems involved are brought back up to full readiness as quickly as possible. The information gathered by the SIB is not releasable to the public, nor is it obtainable through a Freedom of Information Act request. It is simply designed to identify the cause of an accident as quickly as possible to ensure a repeat accident does not occur. The Accident Investigation Board (AIB), on the other hand, conducts their investigation with some portions of the SIB's report but continues its legal process to assign blame. The AIB's reports are made public at the conclusion of the board's investigation. This dual structure could be easily adopted for cybersecurity.

Many companies desire not to release private, internal information on their network designs, known vulnerabilities, and potential or actual breaches due to the fact that much of this information would eventually be made available to the public, and hence to their business competition. In the event of a potential or actual breach of corporate networks, a system similar to the SIB should be activated. The intent of the Cybersecurity Investigation Board (CIB) would be to determine the five W's of the event. Who conducted the breach? Where did the breach occur? When did it occur? What did the perpetrators do while inside the company's networks? Why did this event occur? The CIB would collect this data so that they could quickly share the relevant aspects of the event with the rest of our critical infrastructure owners while keeping the affected company's proprietary information private. Either refusing to release the report or sanitizing the report to ensure that other companies would not be able to piece together any proprietary information and identify the affected company would be a core aspect of this reporting regime.

There would be a need for legislation enacted by the government to protect this type of communication and the identity of the company who provided it. The protected communication system described above coupled with the new legal guarantees should address private sector interests on issues of privacy as well as governmental interests in obtaining information about potential or actual breaches quickly and efficiently.

This type of incentive would cost very little, yet help eliminate the fears of many companies in their decision to cooperate with the U.S. government on cybersecurity.

Another incentive which might bring more of the private sector to the table of critical infrastructure cybersecurity involves lowering the overall costs associated with their cybersecurity programs.

With costs identified as the number one issue businesses contend with regarding their cybersecurity posture (Consortium, 2011), some form of government subsidy would be required to assist in bringing in partners from the business community. What is the best structure for the government to provide a subsidy to those who own and operate our nation's critical infrastructure? With current projections of decreasing federal and local governmental budgets there should be no expectation that any government will have the resources available to provide high levels of funding directed toward cybersecurity; no blank checks in any future cybersecurity partnerships. Yet, with cost as the primary hindrance to effective cybersecurity practices, some amount of funding will need to be made available to these owner/operators. By addressing the private sector's cost interest while simultaneously addressing the government's participation interest there might be a combining of these interests to find a solution.

The U.S. government should create a cybersecurity partnership regime that rewards industry for basic computer network security. This level of cybersecurity is commonly referred to as computer system hygiene. The government should hold businesses accountable for basic security postures like the changing of passwords, patching of operating systems and software applications to remove known vulnerabilities, and the monitoring of their internal systems for potential breaches (Clinton, 2011). The government should also expect companies to pay for these security steps as they are inherently in the best interests of the company to do so. In exchange, once a business has proven they have met the basic standard for cybersecurity, each business would now be allowed to join the private-public partnership, or consortium, for cybersecurity. Becoming a member of the consortium would then open up a wide range of benefits to the company including better access to government information, highly subsidized or free of charge access to research,

development in the cybersecurity field, and access to expert on-site or remote assistance from government employees or agencies. Most importantly, participation in this private-public partnership would ensure the company's reports and other private network information would be handled via the secure communications channel established by Congress in the Cybersecurity Investigation Board process.

The combination of new structure (Cybersecurity Investigation Board) and new financial incentives for bringing a company's systems up to a standard level of cybersecurity defense should address all of the interests of the business community while they debate the merits of joining the private-public partnership (Bissell, 2013). Higher participation from the private sector and more information flowing on cyber-defensive strategies and capabilities would address most of the government's interests as well (Germano, 2014). By successfully addressing each of the participants' interests – both private and public – an increase in not only the potential for a higher level of participation in this private-public partnership for cybersecurity, but also an increase in the chances for success in cybersecurity for our critical infrastructure could be realized.

## CONCLUSION

The threats posed in cyberspace by organized crime, state and non-state actors, and hacktivists among others must be successfully mitigated for the United States to remain safe and secure. All of these cyber threats can be directed against our privately and publically owned and operated critical infrastructure to the advantage of our adversaries. Historically, the business community regarded cooperation with the U.S. government as an obstacle to business efficiency and something to be entered into slowly, if at all. Far too many of the business' interests were not addressed in current private-public partnerships for cybersecurity. The government will need to adapt current partnership models to better address the business community's concerns or face a decision to either mandate compliance via legislation or abandon the quest for cybersecurity partnerships entirely. The future of private-public partnerships does not have to produce such a low return on investments. Molding new partnership models after existing, successful models in other fields can address many

of the interests which remain unanswered today. Changing the structure of government sponsorship and funding of these programs may also help generate the level of participation which could lead private-public partnerships in cybersecurity to become self-sustaining. Companies will need to see more advantages to joining a partnership than they see disadvantages. They need to see not only cost savings but also a return on the cybersecurity investment. Achieving a government standard for their cybersecurity posture will not only get the company to a point where they can protect themselves, but also open up a whole other set of positive opportunities which, in the long run, will lessen their financial burden for their cybersecurity programs.

## AUTHOR

---

**Chris Golden** is a retired senior United States Air Force officer. He spent most of his career flying various airplanes and helicopters and working as a strategic planner. He holds a Bachelor of Science in Computer Science from the University of Miami, a Master of Science in Computer Information Systems from Regis University, and a Master of Arts from the Naval War College. He is currently the director of strategic cybersecurity planning for a major American financial services provider.

## REFERENCES CITED

---

- Bissell, K. (2013, March). A strategic approach to cybersecurity. *Financial Executives International*. Retrieved from: <http://www.financialexecutives.org/>
- Boardman, A.E. & Vining, A.R. (2012, 83.2). The political economy of public-private partnerships and analysis of their social value. *Annals of Public and Cooperative Economics*, 129.
- Bures, O. (2013). Public-private partnerships in the fight against terrorism. *Crime, Law and Social Change*, pp. 429–455. doi: 10.1007
- Busch, N.E. & Givens, A. D. (2013). Realizing the promise of public-private partnerships in U.S. critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, 6, 39–50.
- Business Software Consortium (2011, March 8). *Business improving our nation's cybersecurity through public-private partnerships* [White paper].
- Clinton, L. (2011). A relationship on the rocks: industry-government for cyber defense. *Journal of Strategic Security*, pp. 97–112.
- Germano, J. (2014, October). *Cybersecurity partnerships: a new era in public-private collaboration*. The Center on Law and Security, NYU School of Law.
- lasiello, E. (2012, September 5). Fixing U.S. national cybersecurity: a modest proposal. *Comparative Strategy*, pp. 301–307. doi: 10.1080
- United States Air Force. (2013, November 1). Air force safety and accident board investigations [Fact sheet]. Retrieved from <http://www.acc.af.mil/library/factsheets/factsheet.asp?fsID=2356>
- United States Department of Treasury. (2013). *Report to the President on Cybersecurity Incentives Pursuant to Executive Order 13636*. Retrieved from [http://www.treasury.gov/press-center/Documents/Treasury%20Report%20\(Summary\)%20to%20the%20President%20on%20Cybersecurity%20Incentives\\_FINAL.pdf](http://www.treasury.gov/press-center/Documents/Treasury%20Report%20(Summary)%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf)





# Evolution of Information Security Issues in Small Businesses

Debasis Bhattacharya | Debra A. Nakama

## ABSTRACT

Small businesses often display a lack of concern towards cyber crime and information security problems. This lack of concern usually results in delayed or incorrectly implemented security measures, which increases vulnerability to cyber crime. This paper presents an empirical study of 122 small business owners from the state of Hawaii with regards to their information security. These results are compared with earlier studies conducted in 2000 and 2003. The results of this study showed a significant evolution of information security issues within small businesses. This research suggests that small business leaders need to demonstrate leadership, technical knowledge, and actions to broaden their preparation against a range of information security issues and problems. The findings may be applicable to small business leaders who proactively search for a cost-effective and optimal combination of leadership styles, technologies, and policies that mitigate the evolving threats of cyber crime and information security problems.

## INTRODUCTION

Globalization and increased reliance on the Internet has forced many organizations to rely on computer and networking technology for the storage of valuable company and personal information (Easttom, 2006). Many small businesses have embraced Internet technologies to reach out to their customers, partners, and employees from around the world (Day, 2003). Proliferation of online activity and e-commerce has attracted the attention of existing criminal organizations and a new breed of cyber criminals (Gupta and Hammond, 2005).

Cyber criminals engage in online attacks that exploit vulnerabilities and deficiencies within the cyber defenses of organizations (Szor, 2005). Because of size, resource, and skill constraints, small businesses are often ill-prepared to combat the emerging threats of cyber crime (Ryan, 2000). Small business owners and key employees with effective leadership styles can help prioritize actions needed to combat cyber-crime and mitigate information security concerns (Northouse, 2004). Conversely, ineffective leadership styles can lead to passive or reactive measures against cyber crime, which can lead to business damages and losses (Gupta and Hammond, 2005). Phishing, a deceptive strategy to gain personal information the target might not otherwise divulge, is an increasingly common form of computer attack (Easttom, 2006).

Current research indicates that the information systems of small businesses in the United States are vulnerable to cyber crime (Adamkiewicz, 2005; Baker and Wallace, 2007; O'Rourke, 2003). The problem is small businesses often display a lack of concern towards information security problems (Gupta and Hammond, 2005). This lack of concern usually results in delayed or incorrectly implemented security measures, which increases vulnerability to cyber crime

(Andress, 2003; DeZulueta, 2004). While it may appear that a passive and reactionary approach to computer security threats is economically optimal and cost-effective for many small businesses, the consequences of an actual cyber crime may be potentially damaging to the business.

This study examined the problem by determining whether and to what degree any relationship exists between leadership styles and the level of concern for information security problems. The general population for the study included small businesses located in the state of Hawaii. The results of this study provides small business leaders with information useful in assessing their level of concern and determining which leadership styles are the most effective in mitigating information security problems.

## SECURITY ISSUES WITHIN SMALL BUSINESSES

Cyber crime is not only relevant to large corporations, but to the millions of small businesses in the United States (Gupta and Hammond, 2005). According to the U.S. Small Business Administration and the Small Business Act, a small business is an independently owned entity and not dominant in its field of operation (SBA, 2015). The U.S. Small Business Act also states that the definition of a small business varies by industry. The Office of Advocacy of the U.S. SBA, defines a small business as a business having 500 or fewer employees. This study used U.S. SBA definitions and classifications.

Small businesses play a significant role in the U.S. economy. According to the U.S. SBA's Office of Advocacy, the U.S. had 17,000 large businesses and approximately 25 million small businesses in 2005. Small businesses generated 2.4 times more innovations than large businesses (Easttom, 2006). According to the U.S. SBA, small businesses employ half of all private sector employees and pay half of the total U.S. private payroll.

Small businesses in the U.S. have generated between 60% and 80% of net new jobs annually over the last decade and created more than 50% of non-farm private gross domestic product (SBA, 2015). Economic figures indicate the importance of small businesses

to the U.S. economy and the potential for negative economic impacts from cybercrime (CSI/FBI, 2015). A coordinated cyber threat against small businesses might readily impact a significant section of the U.S. economy (Symantec, 2015). Because small businesses are so important to the U.S. economy, preparation against the evolving threat of cyber crime is important (CSI/FBI, 2015).

In regard to their preparations against cyber crime, small businesses can be divided into three categories. According to the report on the state of small business security (*State of small business security*, 2006), one category consists of “mom and pop” businesses whose business computers also serve as the owners’ home computers. Small businesses in the “mom and pop” category have basic anti-virus and security software in place and rarely rely on skilled professionals for security assistance. The report on the state of small business security also described a second category of small companies with a few hundred employees and a dedicated information technology (IT) staff (CSI/FBI, 2015). According to the U.S. CSI/FBI study (2015) small businesses with a few hundred employees rely on the knowledge and expertise of their key IT personnel for cyber security.

The third and final category included small businesses that outsource most of their security requirements to third-party vendors (*State of small business security*, 2006). According to the report on the state of small business security, vendors provide the level of security needed to prevent cyber crime and enable recovery from security breaches. Small businesses that outsource information security depend upon on the outside vendor’s training and reliability for their security needs (CSI/FBI, 2015). According to the U.S. CSI/FBI study (2015) reliance on an external vendor introduces risks as well as benefits in that it removes the need for a small business to train and retain skilled IT employees to combat cyber crime.

The existing literature on cybercrime and cyber security focuses on the needs of large organizations that have thousands of employees, complex security needs, and large computer systems (Adamkiewicz, 2005). The literature on leadership styles and information security concerns within small businesses is very limited. The literature gap may be due to the evolution of cyber crime, which initially targeted the computer systems of large corporations and government organizations.

As the cybersecurity efforts of large organizations and the government have expanded and improved, the trends of cyber crime have shifted to vulnerable targets like small businesses (Wall, 2005). According to the Symantec Threat Report (Symantec, 2015), cyber criminals increasingly focused on identity theft and fraud for motives of financial gain. The shift in the orientation of cyber criminals over the past few years may help to explain the present literature gap regarding the impact of cyber crime on small businesses.

## STUDY DESIGN

This research study used a quantitative, descriptive, and correlational methodology to investigate a possible relationship between the particular leadership styles of small business owners (independent variables) and the level of concern for information security problems (dependent variables) within small businesses in Hawaii. The study defined a “small business” as one with 500 or fewer employees, according to the United States Small Business Administration (SBA, 2015). This study utilized the Multifactor Leadership Questionnaire (MLQ) instrument (Bass and Avolio, 2004), to assess each company’s leadership style (independent variable) and the Small Business Security Survey instrument (Ryan, 2000) to determine the level of concern for information security problems within each small business (dependent variable).

For the first part of the research, a pilot study was conducted with 10 small businesses that are members of the various chambers of commerce and trade associations within Hawaii. The pilot study participants, randomly selected from the study population, were small business owners who fulfilled the eligibility

criteria of the study population. The randomly selected 10 businesses represented different industries, and had different numbers of employees. Five businesses belonged to the Chamber of Commerce of Hawaii (CoCHawaii, 2015) and five businesses belonged to the Small Business Hawaii (SBH, 2015) trade association.

The second part of the current research involved an online survey of 800 small businesses that, as mentioned previously, are members of the various chambers of commerce and trade associations within Hawaii. Businesses that belong to more than one organization were included only once in the study population in order to avoid duplication. The online survey used two previously validated, reliable, and broadly used research survey instruments (Bass and Avolio, 2004; Ryan 2000).

The third part of this study involved triangulation and the random selection of 10 small businesses from the list of valid respondents to the online survey. Interviews were conducted with 10 businesses to help triangulate the results of the online survey and to confirm or dispute the findings. Triangulation helped reduce the chances for systematic error because the method provided a strategy for obtaining the same information through different methods (Rubin and Babbie, 2005).

## Study Variables

The study contained 14 dependent variables. As shown in Table 1, each variable represented a specific information security problem that a small business may face (Ryan, 2000). Using a Likert scale, the study examined the level of concern for each security problem.

TABLE 1: 14 DEPENDENT VARIABLES

INFORMATION SECURITY PROBLEM	Examples of problems in small businesses.
INSIDER ACCESS ABUSE	Unauthorized login by employees.
VIRUSES	Programs that enter through attachments in email.
POWER FAILURE	Loss of data due to abrupt shutdown of computers.
SOFTWARE PROBLEMS	Vulnerable software due to absence of patches.

TABLE 1 CONTINUED ON NEXT PAGE

TABLE 1: 14 DEPENDENT VARIABLES (CONTINUED)

DATA INTEGRITY	Corruption of customer list or sales data
TRANSACTION INTEGRITY	Corruption of financial transaction with bank
OUTSIDER ACCESS ABUSE	Programs that enter through attachments in email
DATA SECRECY	Confidentiality of payroll information
DATA AVAILABILITY	Availability of access to time sheet data
DATA THEFT	Theft of confidential employee information
DATA SABOTAGE	Intentional destruction of financial data
USER ERRORS	Accidental erasure of data by untrained user
NATURAL DISASTER	Damage to computer systems from floods
FRAUD	Impersonation and deceit used to elicit information

The three independent variables, as shown in Table 2, were the transformational, transactional, and passive-avoidant leadership styles as defined by Bass and Avolio (2004). The study hypothesized that effective leadership styles (the independent variables, listed in Table 2) would foster concern for information security problems (the dependent variables, listed in Table 1) within small businesses.

TABLE 2: THREE INDEPENDENT VARIABLES

LEADERSHIP STYLES	Examples in small businesses
TRANSFORMATIONAL	Visionary, dynamic owner
TRANSACTIONAL	Leader focused on costs/benefits
PASSIVE-AVOIDANT	Absentee, unavailable leader

The research was statistically controlled by five intervening variables derived from the Small Business Security Survey (Ryan, 2000), as shown in Table 3.

TABLE 3: FIVE INTERVENING VARIABLES

VARIABLE NAME	Examples in small businesses
BUSINESS AREA	Industry, as in Agriculture
# EMPLOYEES	Ranges from 1 to 500
ANNUAL REVENUE	\$500,000 to more than \$5 million
# COMPUTERS	Five to more than 100 computers
CONNECTIVITY	Internet, Intranet, E-Commerce etc.

## Hypothesis

The research study employed three statistical hypotheses to measure the relationship(s) among three independent variables (three leadership styles) and 14 dependent variables (information security problems). The  $H_0$  represented the null hypothesis and  $H_a$  the alternative hypothesis. The following hypotheses were tested, based on a quantitative research methodology, to answer the research questions.

### HYPOTHESIS 1

- $H1_0$  There is no relationship between the transformational leadership style score and the level of concern for information security problems within small businesses.
- $H1_a$  There is a relationship between the transformational leadership style score and the level of concern for information security problems within small businesses.

### HYPOTHESIS 2

- $H2_0$  There is no relationship between the transactional leadership style score and the level of concern for information security problems within small businesses.
- $H2_a$  There is a relationship between the transactional leadership style score and the level of concern for information security problems within small businesses.

### HYPOTHESIS 3

- $H3_0$  There is no relationship between the passive-avoidant leadership style score and the level of concern for information security problems within small businesses.
- $H3_a$  There is a relationship between the passive-avoidant leadership style score and the level of concern for information security problems within small businesses.

## Study Results

The study results covered various aspects of information security relevant to small businesses. Table 4 displays the various employees and users who are allowed access to computers and networks within small businesses. The top two groups are full-time and part-time employees, but other user groups like family members and customers may also obtain gain access to computers and networks within small businesses.

TABLE 4: ACCESS TO COMPUTERS AND NETWORKS

N = 122	
ALL FULL-TIME EMPLOYEES	88
PART-TIME EMPLOYEES	47
TEMPORARY EMPLOYEES	26
SOME EMPLOYEES, JOB RELATED	25
CONTRACTORS	22
FAMILY MEMBERS, FRIENDS	19
CUSTOMERS	15
E-COMMERCE PARTNERS	6

Table 5 below displays the information security policies and procedures within small businesses. The top four items include data recovery procedures, information security policies, information security procedures, and computer use and misuse policies.

TABLE 5: INFOSEC POLICIES AND PROCEDURES

N = 122	
DATA RECOVERY PROCEDURES	61
INFORMATION SECURITY POLICY	60
INFORMATION SECURITY PROCEDURES	56
COMPUTER USE AND MISUSE POLICY	54
PROPRIETARY DATA USE AND MISUSE POLICY	47
COMMUNICATIONS USE AND MISUSE POLICY	39
DATA DESTRUCTION PROCEDURES	33
COMPUTER EMERGENCY RESPONSE PLAN	32
BUSINESS CONTINUITY POLICY	25
COMPUTER EMERGENCY RESPONSE TEAM	22
MEDIA DESTRUCTION PROCEDURES	21
INFORMATION SENSITIVITY CODING	14

Table 6 below displays the technologies used by the survey respondents to prevent, detect, and resolve information security problems. The top three technologies are anti-virus software, firewalls, and power surge protectors. The bottom of the list includes security evaluation systems, media degaussers, and dial-back modems.

TABLE 6: INFORMATION SECURITY TECHNOLOGIES

N = 122	
ANTI-VIRUS SOFTWARE	117
FIREWALLS	110
POWER SURGE PROTECTORS	103
DATA BACKUP SYSTEMS	87
SHREDDERS	84
ENCRYPTION	51
SYSTEM ACCESS CONTROL	48
INTRUSION DETECTION	46
FACILITY ACCESS CONTROL	32
REDUNDANT SYSTEMS	31
DATA SEGMENTATION	26
SYSTEM ACTIVITY MONITOR	25
SECURITY EVALUATION SYSTEMS	17
MEDIA DEGAUSSERS	7
DIAL-BACK MODEM	3

Table 7 below displays the importance of several types of data to the respondents of the survey, recorded on an interval scale from 0 (not important) to 5 (extremely important). Customer and privacy data ranked among the top two items in the list, while competitive and market data ranked among the bottom two items in the list. The responses for the importance of customer, privacy, and proprietary data were highly negatively skewed (skewness coefficient < -1.96) indicating the high importance placed by the respondents on these aspects of information security.

TABLE 7: DATA IMPORTANCE

N = 122	MEAN	MEDIAN	SD	SKEW
CUSTOMER DATA	4.25	5.00	1.08	-1.53
PRIVACY DATA	4.13	5.00	1.15	-1.22
PROPRIETARY INFO	3.83	4.00	1.32	-0.74
TRADE SECRETS	3.43	4.00	1.53	-0.36
COMPETITIVE DATA	3.33	3.00	1.38	-0.26
MARKET DATA	3.30	3.00	1.28	-0.26

Table 8 displays the information security issues and problems experienced by the survey respondents within the calendar year 2007. Based on the results, data corruption and problems with virus and malicious software (or malware) topped the list of negative experiences. Abuse of Internet access privileges by employees and problems with reliability in information systems also placed within the top five concerns of survey respondents. Seven respondents reported problems with intrusion to computer systems by outsiders. Seven reported abuse from insiders of information access privileges.

TABLE 8: INFOSEC EXPERIENCES

N = 122	SKEW
DATA CORRUPTED OR PARTIALLY LOST	24
PROBLEMS WITH VIRUS OR MALICIOUS SOFTWARE	22
EMPLOYEES ABUSED INTERNET ACCESS PRIVILEGES	15
PROBLEMS WITH RELIABILITY OF INFORMATION SYSTEMS	15
EXPERIENCED INFORMATION SECURITY INCIDENT	8
OUTSIDER BREAK IN TO INFORMATION SYSTEM	7
INSIDER ABUSED INFORMATION ACCESS PRIVILEGES	7
VICTIM OF FRAUD	5
LOST MONEY DUE TO INFORMATION SECURITY PROBLEM	4
VICTIM OF A NATURAL DISASTERS	4
COMPUTER EQUIPMENT STOLEN	4
PROPRIETARY DATA STOLEN	3
SECRET INFORMATION DIVULGED	3

## Key Findings on Leadership and Security

The theoretical framework of this research study was based on the full range leadership model of Bass and Avolio (2004). The study used the MLQ instrument that includes a Likert scale to measure three specific leadership styles (defined here as independent variables) of small business owners. The MLQ instrument assesses three leadership styles by investigating nine behavioral factors. Through extensive factor analysis in 2003, Bass and Avolio have identified the five behavioral factors of the transformational leadership style as follows: idealized attributes (IA), idealized behaviors (IB), inspirational motivation (IM), intellectual stimulation (IS), and individualized consideration (IC).

Through confirmatory factor analysis, Bass and Avolio have also identified two behavioral factors of transactional leadership style: contingent reward (CR) and management-by-exception (active) (MBEA). Finally, their factor analysis determined the two behavioral factors of laissez-faire or passive-avoidant leadership style: passive management-by-exception (passive) (MBEP) and laissez-faire (LF).

The findings indicated that transactional leadership style is significantly related to 11 out of 14 information security problems. This implies that the higher the level of transactional leadership style score, the higher the level of concern for 11 information security problems.

The transactional leadership factor of Management by Exception Active (MBEA) is significantly related to 10 out of 14 information security problems. This implies that the higher the practice of active management by exception, the higher the level of concern for 10 information security problems.

Seven out of 14 information security problems were related to more than one leadership factor.

Using stepwise multiple regression analysis, the transformational factor of Idealized Influence Attributes (IIA) and the transactional factor Management by Exception (MBEA) were the best predictors for the seven information security problems. This implies a combination of transformation and transactional leadership styles to prepare against seven common security problems.

The findings also indicated that transformational leadership style was significantly related to the level of concern for two information security problems, and passive-avoidance leadership was related to a single information security problem. Using the Pearson product-moment correlation, there is a statistically significant ( $p \leq 0.05$ ), positive correlation between transformational leadership style score and the level of concern for two (out of 14) information security problems. These two problems are data secrecy and data availability. Thus, the null hypothesis  $H1_0$  is rejected.

Likewise, there is a statistically significant ( $p \leq 0.05$ ), positive correlation between transactional leadership style score and the level of concern for 11 (out of 14) information security problems. Therefore, the null hypothesis  $H2_0$  is strongly rejected.

Finally, there is a positive correlation between passive-avoidance leadership style score and the level of concern for one (out of 14) information security problems, power failure. While the null hypothesis  $H3_0$  is rejected, it is not as strongly rejected as  $H1_0$  and  $H2_0$ .

## EVOLUTION OF SECURITY ISSUES AND CONCERNS

The study results of 2008 (N=122) were compared to similar studies, using the same survey, conducted by Ryan (2000) and Gupta (2003). The study by Ryan covered small businesses in the United States with particular focus on businesses located in the state of Maryland. 209 responses were collected from the study by Ryan (N=209). Gupta focused on the Chamber of Commerce in the South Eastern United States and collected responses from 138 small business (N=138). Table 9 describes the changes in access to computers and networks over the years for small businesses, with sharp growth in usage over the years for all employees, contractors and family members.



TABLE 9: ACCESS TO COMPUTERS AND NETWORKS

	2000	2003	2008
ALL FULL-TIME EMPLOYEES	57.4%	49.3%	72.1%
PART-TIME EMPLOYEES	17.2%	18.8%	38.5%
TEMPORARY EMPLOYEES	21.3%	8.7%	21.3%
SOME EMPLOYEES, JOB RELATED	31.6%	49.3%	20.5%
CONTRACTORS	6.7%	3.6%	18%
FAMILY MEMBERS, FRIENDS	24.4%	2.2%	15.6%
CUSTOMERS	6.2%	6.5%	12.3%
E-COMMERCE PARTNERS	1.9%	0.7%	4.9%

Table 10 displays the changes in information security policies and procedures within small businesses. The results suggest an increase in policies and procedures in most categories, especially in the areas of information security policy and procedures, and computer misuse and data destruction.

TABLE 10: INFOSEC POLICIES AND PROCEDURES

	2000	2003	2008
DATA RECOVERY PROCEDURES	39.7%	47.1%	50%
INFORMATION SECURITY POLICY	30.6%	40.6%	49.2%
INFORMATION SECURITY PROCEDURES	23%	32.6%	45.9%
COMPUTER USE POLICY	24.9%	42.8%	44.3%
PROPRIETARY DATA USE POLICY	18.2%	26.1%	38.5%
COMMUNICATION USE POLICY	13.9%	25.4%	32%
DATA DESTRUCT PROCEDURES	12.9%	21%	27%
COMP EMERGENCY RESPONSE PLAN	13.4%	18.8%	26.2%
BUSINESS CONTINUITY POLICY	21.5%	23.9%	20.5%
COMP EMERGENCY RESPONSE TEAM	7.18%	13.8%	18%
MEDIA DESTRUCTION PROCEDURES	6.7%	9.4%	17.2%
INFO SENSITIVITY CODING	13.4%	25.4%	11.5%

Table 11 displays the changes in the technologies used by the survey respondents to prevent, detect, and resolve information security problems. The results indicate a sharp increase in the use of firewalls, shredders, and intrusion detection systems, but a surprising decline in the use of system access control and redundant systems.

**TABLE 11: INFORMATION SECURITY TECHNOLOGIES**

	2000	2003	2008
ANTI-VIRUS SOFTWARE	87.1%	56.5%	95.9%
FIREWALLS	25.8%	42.8%	90.2%
POWER SURGE PROTECTORS	70.3%	79.7%	84.4%
DATA BACKUP SYSTEMS	75.1%	65.2%	71.3%
SHREDDERS	44.5%	48.6%	68.9%
ENCRYPTION	25.4%	18.8%	41.8%
SYSTEM ACCESS CONTROL	72.7%	58%	39.3%
INTRUSION DETECTION	22.5%	25.4%	37.7%
FACILITY ACCESS CONTROL	14.4%	17.4%	26.2%
REDUNDANT SYSTEMS	45.5%	34.8%	25.4%
DATA SEGMENTATION	28.7%	23.9%	21.3%
SYSTEM ACTIVITY MONITOR	15.8%	21%	20.5%
SECURITY EVALUATION SYSTEMS	11.5%	8.7%	13.9%
MEDIA DEGAUSSERS	3.3%	0.7%	5.7%
DIAL-BACK MODEM	10%	8.7%	2.5%

Table 12 displays the changes in the importance of several types of data to the respondents of the survey, recorded on an interval scale from 0 (not important) to 5 (extremely important). The results indicate a steady increase in the importance of customer, privacy, proprietary, trade secrets, and competitive data.

**TABLE 12: DATA IMPORTANCE**

	2000	2008
DATA CORRUPTED OR PARTIALLY LOST	28.7%	19.7%
PROBLEMS WITH VIRUS/MALICIOUS SW	20.6%	18.0%
EMPLOYEES ABUSED INTERNET PRIVILEGES	6.7%	12.3%
PROBLEMS WITH RELIABILITY OF IS	18.2%	12.3%
EXPERIENCED I.S. INCIDENT	8.6%	6.6%

Table 13 displays the changes in information security issues and problems experienced by the survey respondents in two separate studies conducted in 2000 and 2008. The results indicate that data corruption and problems with viruses and malicious software remain the highest concerns for small businesses. The results also indicate a sharp rise in abuse of Internet privileges.

TABLE 13: INFOSEC EXPERIENCES

	2000	2008
DATA CORRUPTED OR PARTIALLY LOST	28.7%	19.7%
PROBLEMS WITH VIRUS/MALICIOUS SW	20.6%	18.0%
EMPLOYEES ABUSED INTERNET PRIVILEGES	6.7%	12.3%
PROBLEMS WITH RELIABILITY OF IS	18.2%	12.3%
EXPERIENCED IS INCIDENT	8.6%	6.6%
OUTSIDER BREAK-IN TO I.S.	1.9%	5.7%
INSIDER ABUSED INFO PRIVILEGES	3.3%	5.7%
VICTIM OF FRAUD	3.8%	4.1%
LOST MONEY DUE TO I.S. PROBLEM	9.1%	3.3%
VICTIM OF A NATURAL DISASTER	3.3%	3.3%
COMPUTER EQUIPMENT STOLEN	2.9%	3.3%
PROPRIETARY DATA STOLEN	1.0%	2.5%
SECRET INFORMATION DIVULGED	1.9%	2.5%

## IMPLICATIONS FOR SMALL BUSINESSES

These study findings support the model that transformational leadership augments transactional leadership in predicting effects on employees. Bass and Avolio (2004) supported the model with evidence and noted that transactional leadership provides a basis for effective leadership, but a “greater amount of Extra Effort, Effectiveness, and Satisfaction is possible from employees by augmenting transactional with transformational leadership” (p. 22).

The study also highlights the need to complement the benefits of transformational and transactional leadership styles with effective policies and updated technologies that mitigate information security problems. Small businesses cannot rely primarily on basic technologies such as anti-virus software, firewalls, and power surge protectors — the top three technologies in Table 6 — to protect against cybercrime. Likewise, small businesses cannot rely primarily on basic data recovery procedures and information security policies and procedures for protection against cybercrime.

### Recommendations

The first recommendation for small business leaders is to introduce a systematic and consistent system of leadership assessment within their organization. The Multifactor Leadership Questionnaire (MLQ), available from Mind Garden Inc. (2008), is a valid and reliable survey instrument for assessing leadership styles within a small business. The results of this research study highlight the importance of three leadership factors that are components of transformational and transactional leadership styles. These leadership factors are Idealized Influence Attributes (IIA), Contingent Reward (CR), and Management-by-Exception Active (MBEA). Small business leaders can evaluate their scores on these three leadership factors by using the MLQ (Rater Form) with their subordinates.

The second recommendation is for small businesses to conduct an audit of their information security. A website (ReadyBusiness, 2015) and guide published by the US Department of Homeland Security (2015) provides a detailed checklist to conduct security assessments within small businesses. Additional detailed guides from NW3C (2015) and

TABLE 14: CYBERCRIME LEADERSHIP, TECHNOLOGY AND POLICY

SECURITY PROBLEM	Leadership Style	Technology and Policy to Augment Leadership Style
INSIDER ACCESS ABUSE	Transactional	Computer Emergency Response Team, Encryption Technology
VIRUSES	Transactional	Anti-virus software, Computer Emergency Response Plan
DATA INTEGRITY	Transactional	Intrusion Detection Systems, Computer Use and Misuse Policy
OUTSIDER ACCESS ABUSE	Transactional	Intrusion Detection Systems
DATA SECRECY	Transformational	Information Security Policy, System Activity Monitors, Anti-virus software
DATA AVAILABILITY	Transactional	Computer Use and Misuse Policy
DATA THEFT	Transactional	Computer Emergency Response Team, Anti-virus software, System Activity Monitors
DATA SABOTAGE	Transactional	Computer Emergency Response Team, Intrusion Detection Systems
USER ERRORS	Transactional	Computer Emergency Response Team, Anti-virus software
NATURAL DISASTER	Transactional	Computer Emergency Response Plan
FRAUD	Transactional	Computer Emergency Response Team

ISO/IEC (2015) provides a risk audit for very small businesses, with 10 or less employees, who were the primary respondents for this research study.

The third recommendation is to utilize a combination of leadership styles, technology and policy to combat specific security problems and concerns, as displayed in Table 14. It should be noted that small businesses should adopt a cost-effective and practical approach to security solutions. For example, deploying an internal computer emergency response team (CERT) or installing an Intrusion Detection System (IDS) may not be realistic for many small businesses. However, small businesses could rely on security training, outsourcing solutions and computer use and misuse policies to alleviate the security threats. The key is that one leadership style is not applicable to all security problems and that technology and policy solutions need to be augmented with leadership and knowledge

### Suggestions for Future Research

Based on the study findings, two suggestions are offered for further research. The first suggestion is to conduct additional studies in several small and large states in the United States and broaden the sample population. This expansion may result in findings that are based on experiences of small business in various situations that are not relevant to the state of Hawaii. Additional research may be conducted in overseas countries that contain small businesses with profiles similar to those of small businesses in the United States. This global exposure will provide researchers with insight into global security problems and issues.

Another suggestion is to conduct similar studies on an ongoing basis for the next decade. Given the evolving nature of cybercrime and information security, the attitudes and exposures of small businesses vary over

time. As such, regular studies conducted over a long period of time will provide researchers with details on trends and new issues. The results from these studies will provide researchers with a comprehensive evaluation of the growth and evolution of cyber crime and the abilities to combat it.

## CONCLUSIONS

This research study is socially significant in its finding that leadership styles are statistically significant when it comes to mitigating information security issues and concerns within small businesses. Small business leaders are preoccupied with everyday business issues and concerns and often display a lack of concern towards information security problems. A lack of concern usually results in delayed or incorrectly implemented security measures, which increases vulnerability to cyber crime (Andress, 2003).

This research has demonstrated the need for effective transactional and transformation leadership styles that will enable small business leaders to prioritize their efforts to mitigate cyber crime. An optimal combination of leadership styles, security policies, and technology enable small businesses to prevent and combat cyber crime.

## REFERENCES CITED

- Adamkiewicz, S. L. (2005). *The correlation between productivity and the use of information security controls in small businesses*. The George Washington University, United States—District of Columbia.
- Andress, A. (2003). *Surviving security: How to integrate people, process and technology*. New York: Auerbach Publications.
- Baker, W. H., & Wallace, L. (2007). Is information security under control? *IEEE Security & Privacy*.
- Bass, B. M., & Avolio, B. (2004). The multifactor leadership questionnaire: Sampler set.
- CoCHawaii. (2015). The Chamber of Commerce of Hawaii. Retrieved May 26, 2011, from <http://www.cochawaii.com/>.
- CSI/FBI. (2015). *Computer Crime and Security Survey XI Annual*. Retrieved September 3, 2015, from [http://i.cmpnet.com/gocsi/db\\_area/pdfs/fbi/FBI2006.pdf](http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf).
- Day, K. (2003). *Inside the security mind: Making tough decisions*. Upper Saddle River, NJ: Prentice Hall.
- DeZulueta, M. (2004). *A novel neural network based system for assessing risks associated with information technology security breaches*. Florida International University, United States—Florida.
- Easttom, C. (2006). *Computer security fundamentals*. Upper Saddle River, NJ: Prentice Hall.
- Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security*, 13(4), 297.
- Homeland Security. (2015). Tools for small business. Retrieved September 3, 2015, from [http://www.ntsbdc.org/docs/sba\\_homeland\\_security.pdf](http://www.ntsbdc.org/docs/sba_homeland_security.pdf)
- ISO/IEC. (2015). ISO/IEC 17799:2005 Information technology—security techniques. Retrieved September 3, 2015, from [http://www.iso.org/iso/information\\_security](http://www.iso.org/iso/information_security).
- MindGarden. (2015). Multifactor Leadership Questionnaire. Retrieved September 3, 2015, from <http://www.mindgarden.com/products/mlq.htm>
- Northouse, P. G. (2004). *Leadership: Theory and practice*. Thousand Oaks, CA: Sage.
- NW3C. (2015). National White Collar Crime Center. Retrieved May 26, 2015, from <http://www.nw3c.org/>.
- O'Rourke, M. (2003). Cyberattacks prompt response to security threat. *Risk Management*, 50(1), 8.
- ReadyBusiness. (2015). Ready.Gov—small business readiness. Retrieved September 3, 2015, from <http://www.ready.gov/business/index.html>.
- Rubin, A., & Babbie, E. (2005). *Research methods for social work* (5th ed.). Belmont, CA: Brooks/Cole-Thomson.
- Ryan, J. J. C. H. (2000). *Information security practices and experiences in small businesses*. The George Washington University, United States—District of Columbia.
- SBA. (2015). US Small Business Administration. Advocacy Small Business Statistics and Research. Retrieved September 3, 2015, from <http://app1.sba.gov/faqs/faqindex.cfm?areaid=24>.
- SBH. (2015). Small Business Hawaii. Retrieved September 3, 2015, from <http://www.smallbusinesshawaii.com/SBAbout.html>.
- The state of small business security in a cyber-economy: Hearing before subcommittee on regulatory reform and oversight of the committee on small business*, US House of Representatives, 109th Congress Second Sess. (2006).
- Symantec. (2015). Small and mid-sized business products. Retrieved September 3, 2015, from <http://www.symantec.com/smb/products/index.jsp>.
- Szor, P. (2005). *The art of computer virus research and defense*. Upper Saddle River, NJ: Symantec Press.
- Wall, D. S. (2005). The internet as a conduit for criminal activity. In A. Pattavina (Ed.), *Information technology and the criminal justice system*. Thousand Oaks, CA: Sage Publications.

## AUTHORS

---

**Debasis Bhattacharya** ([debasisb@hawaii.edu](mailto:debasisb@hawaii.edu)) is currently a faculty member at the University of Hawaii Maui College and is responsible for the Applied Business and Information Technology program. Dr. Bhattacharya has worked in the software industry for 27 years for large mainland corporations such as Oracle and Microsoft Corporation. He has lived on Maui, Hawaii, for the past 13 years and has been actively researching the information security needs of small business owners since 2008.

**Debra A. Nakama** ([debran@hawaii.edu](mailto:debran@hawaii.edu)) has more than two decades of experience implementing federal workforce and economic development career pathways from middle school to community college to the workforce. Over the last 10 years, with the Maui Educational Consortium, a K–16 cross-level teachers and administrators group, Dr. Nakama has focused on designing evaluations using longitudinal intervention strategies as a way of informing K–12 and college stakeholders of effective methods for increasing the college matriculation rates of underachieving populations.

# Hybrid Implementation of Flipped Classroom Approach to Cybersecurity Education

Aparicio Carranza | Casimer DeCusatis

## ABSTRACT

A flipped classroom is a pedagogical model in which the typical lecture and homework/lab portions of a course are reversed. Students review course content each week on their own time, and then devote class time with an instructor to a discussion of the prepared material and hands-on practice exercises. The notion of a flipped classroom has been studied extensively, and draws on such concepts as active learning, student engagement, and hybrid course design. We discuss the cybersecurity teaching for Computer Engineering Technology students at New York City College of Technology (NYCCT), of the City University of New York (CUNY) using a version of the flipped classroom. NYCCT is an open institution and is a federally designated Hispanic Serving Institution (HSI) with a significant population of women and other groups which are under-represented in IT fields. A version of the flipped classroom has proved to be an effective way of engaging the students in the study of computer security. The courses have unique requirements because students need an environment to practice their hacking skills which is isolated from the outside world (a virtual lab setting is used for this purpose). Individual students also prepare two short case studies on cybersecurity topics of their choosing and a semester-long research project. Since this is an elective special topics course, there are no traditional exams or tests. We employ a hybrid model in which alternate class meetings are met using Skype. We present a detailed discussion of the methods used in this course and feedback from students with their recommendations for broader adoption of this approach.

## INTRODUCTION

There has been a significant increase in the number, severity, and complexity of attacks against computer infrastructure in recent years. For example, the number of vulnerabilities catalogued by the NIST database of Common Vulnerabilities and Exposures (VCE) increased 30% between 2014 and 2015, including nearly 10,000 new incidents in the past year alone (Cisco 2014 annual security report). Given the fundamental importance of a secure computing environment for many lines of business, cybersecurity has been widely recognized as a national priority by such organization as the Department of Homeland Security, NSF, NIST, and the Office of the President of the United States (White House, 2015; Obama, 2015; Exec. Order No. 13636 (2013); Presidential Policy Directive, 2013). Cybersecurity has also been recognized as a critical asset in most leading academic, industry, and government organizations. Degree programs and specializations in cybersecurity are widely offered as part of the undergraduate portfolio by many computer science and information technology (IT) programs worldwide, according to the National Initiative for Cybersecurity Careers and Studies and other sources (National Initiative for Cybersecurity Careers and Studies, 2015; Corno, 2014; IT Career Finder, 2014–2015; The National Initiative for Cybersecurity Education, 2015; ACM Curricula Recommendations, 2015). Without additional education programs in this field, the IT industry will continue to face a shortfall of between one and two million trained, certified security professionals within the next five years (Corno, 2014; IT Career Finder, 2014–2015). Current analyst reports note that hiring demand for security experts has increased steadily over the past three years in both government and private sector positions and that security is the only area of certified IT skills that has never had a negative quarter since 2008 (IT Career Finder, 2014–2015).

The National Institute for Cybersecurity Education has recently encouraged the formation of new formalized cybersecurity education programs (The National Initiative for Cybersecurity Education, 2015). The Association of Computer Machinery (ACM), in work supported by the National Science Foundation, has also produced curriculum recommendations for cybersecurity education (ACM Curricula Recommendations, 2015). A recent National Science Foundation workshop emphasized the need for better security education in undergraduate computer science programs and the need to treat cybersecurity as a foundational, multi-disciplinary skill (much like courses in operating systems). This report cites a particular need to encourage increased participation from traditionally under-represented students in this field.

Conventional approaches to information security education are hard pressed to prepare enough students with the right skills to meet rapidly growing demand in this field. While industry certification programs are available, they tend to emphasize memorization and repetition over a deeper cognitive framework or understanding. It can be quite challenging to prepare students for IT careers in this rapidly evolving field or to integrate these offerings into a more traditional undergraduate engineering curriculum. More hands-on experience is desirable since students must be prepared to deal with not only existing security threats but also new and increasingly complex exploits which emerge more frequently each year. However, students require a secure, isolated environment in which to practice their security skills without risking damage to the campus data centers or servers on the Internet. Until recently, it was not cost effective to provide students with access to real world examples of IT infrastructure. There have been several reports about the need to reform engineering and computer science education (Wilcox, Wilcox, 2013), as well as reports on the transformative power of early curriculum redesign efforts in this field. As part of this transformation, the gap between teaching methods and practitioner's skills can be addressed, at least in part, through new teaching models such as flipped classrooms (Bishop, Verleger, 2013; Sams, Bergmann, Daniels, Bennet, Marshall, Arfstrom, 2014; Carranza, DeCusatis, 2015) and increased academic partnerships, the latter having been shown to help foster interdisciplinary education.

In this paper, we discuss a new undergraduate program in cybersecurity for Computer Engineering Technology students using the hybrid flipped classroom approach. This program was recently piloted at the New York City College of Technology (NYCCT), which is part of the City University of New York (CUNY) system, an environment with a significant population of economically challenged, nontraditional students. We have also implemented a variation of this approach at Marist College, a private liberal arts school in upstate New York. We discuss implementation of these approaches, including not only technical skills training but also the promotion of critical thinking, systems analysis, and interpersonal skills. A version of the flipped classroom has proved to be an effective way of engaging students in the study of computer security. We present a detailed discussion of the methods used, feedback from students and faculty, and recommendations for broader adoption of this approach.

## CYBERSECURITY EDUCATION GOALS

We have implemented cybersecurity education programs at two major institutions, NYCCT and Marist College. Marist is a private, co-educational, liberal arts college founded in 1905 by the religious order of the Marist Brothers and subsequently accredited by the state of New York in 1929. Organizations such as the Princeton Review and U.S. News and World Report consistently rank Marist as among America's best colleges, best college values, and best regional schools in the country. Recent enrollment includes about 5,000 undergraduates and 1,000 graduate students. Marist maintains foreign study programs in 26 countries, and over 50% of undergraduate students include some form of international study program in their degree program (significantly higher than the national average of about 7%). The School of Computer Science and Mathematics is the largest and fastest growing school within the college. In January 2013 the State of New York approved a \$3 million grant to establish the Cloud Computing & Analytics Center (CCAC) at Marist College. As part of this effort, Marist has established a test bed for next generation cloud computing research, and also hosts cloud workloads for local businesses and government organizations. Marist has recently begun a significant educational



and research program devoted to cybersecurity, including various types of security education and training, developed in collaboration with the School of Criminal Justice and various industry partners.

NYCCT, or City Tech, is the designated senior college of technology within the 24-unit City University of New York (CUNY), the largest urban public university system in the nation. The National Science Foundation ranks City Tech third nationally in the number of associate-level science and engineering degrees awarded to Black students, 23rd in degrees awarded to male students, and 48th in degrees awarded to women. Fall Semester 2013 student enrollment was 16,803, of whom 35% attended part-time. The student body reported 138 different countries of origin. As an open access institution, City Tech's historic mission has been to offer opportunities for educational advancement to students regardless of financial circumstances or prior academic achievement. The college is a federally designated Hispanic Serving Institution (HSI). The primary goal for CUNY students concentrating on cybersecurity is to provide the background necessary to enable them to become successful IT practitioners, including information security administrators, architects, and testers, within the context of a broader knowledge of Computer Engineering. We are particularly interested in local job opportunities in the nearby Wall Street financial district, where many employers are actively deploying cloud computing environments and have a significant interest in data security. There are a limited number of available hours in our curriculum that are not previously dedicated to other requirements, so it is important to prioritize key concepts and skills for any new course offering. The Computer Engineering curriculum at City Tech allows students to earn a two year Associate of Applied Science degree in Electro-Mechanical Technology. After completing two years of additional coursework, students can earn a Bachelor of Technology degree in Computer Engineering Technology. These programs are Accreditation Board for Engineering and Technology, Inc. (ABET) accredited. Cybersecurity is included as an elective course component during the junior/senior year.

The fundamental concepts which students should understand after successfully completing a course of study in cybersecurity include the following:

- Framework and key concepts based on established cybersecurity certifications
- Hands-on experience in cyber defense tools and techniques
- Security governance and ethics
- Penetration testing of data center servers, storage, and networks
- Implementing data confidentiality, integrity, and authentication
- Managing mobile device and wireless security
- Programming security scripts and compiled code based on open industry standards, and contributing to open source software projects
- Understanding recent use cases in information security as a basis for future threat assessment

## FLIPPED CLASSROOM APPROACH

The so-called flipped classroom is a pedagogical model in which the typical lecture and homework elements of a course are reversed (Bishop, Verleger, 2013; Sams et al. 2014). There is no single model for the flipped classroom. The term is widely used to describe almost any class structure that provides students with resources (such as reading assignments) which are to be studied prior to regular class meetings. The value of this approach lies in re-purposing class time into a workshop where students can ask questions about the class resources and interact with their peers in hands-on activities. Instructors function as coaches or advisors, encouraging students to individually pursue their interests and collaborate on class projects. This approach draws from other educational concepts such as active learning, student engagement, and hybrid course design. Fully realized, this approach can provide a radical change in the classroom dynamic. A number of higher education institutions have recently begun experimenting with the flipped classroom approach, including Harvard, Penn State, and Algonquin College (Sams et al. 2014).

In a traditional lecture, students often try to capture what is being said at the same instant the speaker makes a comment. Students can't stop to reflect on

what's being said, and may miss significant points in their haste to transcribe the instructor's words. In a flipped classroom, students control the rate at which they absorb and reflect upon new materials. This may be particularly effective for students with accessibility concerns, or for whom English is a second language. Devoting class time to conceptual understanding may give instructors a better chance to observe and correct student errors. Collaborative or group projects further these goals by encouraging social interaction among students, making it easier for students of varying skill levels to support each other.

Of course, there are potential pitfalls associated with a flipped model. An effective flip requires careful preparation by the instructor, particularly in the early part of the course. Instructors should also seek out additional opportunities to interact with their students outside the traditional classroom. Instructors give up their traditional front-of-the-class position in favor of a more collaborative and cooperative role. Student roles change as well, as they become more active participants in their own learning experience. The flipped model gives students more opportunities to experiment while placing more of the responsibility of learning on the student. Students and instructors may be uncomfortable in these new roles, or may not appreciate the value of hands-on exercises. On the other hand, when a flip is done well, it can shift the priorities of the class from merely covering material to working towards the achievement of deeper insights which can be applied to new situations beyond the scope of the current course examples. We will discuss variations on the flipped classroom model which attempt to preserve many of its strengths while overcoming some of its known weaknesses.

## INSTRUCTIONAL MATERIALS

Marist College offers an Introduction to Cybersecurity course using the textbook *Elementary Information Security* by R. Smith (second edition, 2015). While this is a large book for a one semester course (over 16 chapters), it provides students with ample opportunity to conduct independent reading assignments. Marist also offers courses in Hacking and Penetration Testing (based on S. Oriyano's book, second edition, 2015) and Mobile Security (based on J. Dougherty's book, second edition, 2014). Prerequisites

for these courses include classes such as Introduction to Programming, Data Communication, and Internetworking. The introductory course was offered for the first time in fall 2015, with an enrollment of 30 students.

The required textbook for the NYCCT Cybersecurity class is *Penetration Testing: A Hands-On Introduction to Hacking* by G. Weidman (2014). This course does not assume any prior knowledge of Windows, Linux, or computer networking, although an introductory programming course is prerequisite (such as C or C++). As a supplemental text, the course also uses *Applied Information Security, a Hands-on Guide to Information Security Software* by R. Boyle and J. Proudfoot (2014). The supplemental text is used primarily for teaching Windows security and command line management techniques. Currently the course is offered as an elective for undergraduate junior and senior students in computer engineering technology. The course was offered for the first time in 2014 with an enrollment of 22 students.

For computer security labs, it is essential to provide students with an isolated, "sandbox" environment to practice their hacking skills. There is always concern that a student will decide to experiment on their own using the campus network or the Internet, which introduces liability issues for the college and instructor as well as the potential for students to do significant damage (either accidentally or intentionally). For the Marist courses, labs are conducted in a secure cloud computing environment and isolated from the rest of the campus network. For the NYCCT course, students perform labs on their own computers which are not allowed to access the Internet from campus. At the start of both courses, students are introduced to the ethical conduct standards and practices published by the IEEE and ACM, which they are expected to follow throughout the course.

## FLIPPED CLASSROOM ENVIRONMENT

NYCCT has implemented a more classic flipped classroom approach following an initial period of two weeks in which their computers are provisioned with the required security environment tools. Students receive instruction on how to set up a VMware virtual environment which is used for the rest of the course,

including a review of basic programming techniques a general introduction to Linux and a specific introduction to Kali Linux. The desktop version of VMware Player, available for free on Windows and Linux Operating Systems, is used. Kali Linux is a Debian-based Linux distribution that comes with a wide variety of pre-installed security tools that are employed throughout the course. All of the students' virtual machines (VMs) are placed on the same virtual network using a bridged connection with static IP addresses (the same connection as the host system without the default network address translation normally enabled on Kali Linux). Kali Linux includes the Ming C compiler and the GNU Compiler Collection (GCC) for compiling code to run on Windows systems, as well as interpreters for Python and Pearl. (For example, students can write exploits in Python shell scripts for this course.) The course also uses other free software not included in the Kali Linux distribution. This includes the open source version of the de facto industry standard Metasploit Framework, which makes it quick and easy to explore well over a thousand known system vulnerabilities. Other software used in this class includes the Hyperion encryption program (to bypass antivirus software), Veil-Evasion (which creates payload executables capable of bypassing common antivirus solutions), Ettercap (a tool for man-in-the-middle attacks), and Tenable Security's Nessus Home vulnerability scanner. Optionally, Android SDK emulators are used for mobile security testing. Students create custom-build target machines to simulate vulnerabilities often found in real-world systems using Windows 7, Windows 8, Ubuntu, Fedora, or CentOS.

Following the initial setup period at NYCCT, teams of between two and four students are expected to complete weekly reading assignments and submit completed lab reports. There are no fixed deadlines on lab project submission, although students are provided with a recommended timetable and are required to complete nine labs during a 15 week semester (this accounts for 50% of their total grade). Class meetings are used to discuss the material and help students work their way through the curriculum. In this course, students are encouraged to seek out the instructor at any time using Skype video conferencing tools to discuss their progress. In this way, student/instructor interaction is not limited to weekly class meetings and students can interact with the instructor individually

or in small groups. In addition to lab assignments, students complete two case studies during the semester. Each case study is a short paper (typically five pages, though there is no upper limit) on a topic approved by the instructor which is of interest to the student. Each case study is worth 10% of the student's final grade. Finally, 30% of the student's final grade is based on a research paper and oral presentation to the class at the end of the semester. Research papers are longer than case studies, typically 8–15 pages (though again, there is no upper limit) and are accompanied by a 15–30 minute oral presentation which is recorded to provide feedback to the students. Examples of student research paper topics include analysis of the Heartbleed Exploit, cognitive security based on the Turing Test, and computer forensics using the Kane software package. Students benefit from hearing and critiquing oral presentations on a variety of topics, so the instructor assures that each group of students has a unique subject to present.

Response to this new course and format has been overwhelmingly positive. Initially a few students expressed concern about the lack of traditional midterm and final exams. However, such concerns were quickly offset by the student's enthusiasm for this topic and the flexibility to choose subjects which they found interesting for their case studies and final projects. Student evaluation forms completed at the end of the course contained many positive comments and not a single complaint on the lack of conventional exams; student write-in comments cited this course as among the best classes they have ever taken. The initial class of students has reported strong interest from industry employers in this field and high placement rates for the initial group of students. Students are encouraged to pursue novel, open source implementations or contributions to the Kali Linux libraries and submit their work for presentation at local professional conferences. This not only provides excellent experience for the students and promotes interpersonal communication skills, but also exposes them to potential employers in the region. Several students from this class went on to present their research projects at IEEE sponsored technical conferences (Carranza, Carranza, 2014; Zafar, Carranza, 2014; Flores, Piure, Carranza, 2014; Estrella, Carranza, DeCusatis, 2015). Several students are also exploring collaborations with other academic research institutions, including the New York State Cloud Computing and Analytics

Center at Marist College. The instructor evaluation reported higher than normal workload during the first 2–3 weeks of the course and assessed their workload for the rest of the course as being consistent with a traditional stand-up lecture/exam format.

## HYBRID FLIPPED CLASSROOM ENVIRONMENT

While the classic flipped classroom model has proven successful during initial trials at NYCCT, there are also some potential drawbacks. When introducing new concepts such as encryption and public key cryptography, students can benefit from a lecture which presents the concepts from a point of view different from the textbook, prompting the students to ask questions which they may not have otherwise considered. This includes making explicit connections with different parts of the curriculum which might otherwise be missed by students working independently. At Marist College and NYCCT, we have explored a hybrid approach which incorporates some of the independent learning benefits from a fully flipped classroom with the benefits of more traditional classroom lectures.

For example, a student with a background in Java programming who independently studies the security implications of buffer overflows may wonder if the Java stack and heap are subject to overflow attacks. The simple answer (which the student would find on their own with a short review of online resources) is that a memory managed language such as Java mandates automatic array bounds checking, throws an exception when a method attempts to access array elements that are out of bounds, and then a try-catch loop handles the exception, making buffer overflows impossible. In many classrooms, this would be the end of the discussion. However, this question provides a teachable moment: the instructor should expand on the original question and lead the student to use their own Java experience to consider whether other circumstances might lead to security risks in Java array handling. For example, if the Java Virtual Machine (JVM) or Java Development Environment (JDE) is written in another language such as C++, the JVM or JDE might be vulnerable to buffer overflows. Calling the Java Native Interface provides unmanaged pointer access. Further, there may be errors in the code which incorrectly handle the array-out-of-bounds exception;

if an attacker can trigger enough exceptions by entering invalid inputs, an effective denial of service attack can be launched. In this manner, a prepared instructor can introduce new concepts (such as attack vectors for denial of service attacks) while reinforcing the textbook answer on Java buffer overflow attacks. There is value in preparing brief lecture notes along these lines and introducing the topic during class even if the students fail to ask the original question.

This example illustrates the benefits of a so-called hybrid flipped classroom for cybersecurity education. While students are still held responsible for independent learning from the class resources, time is allocated from each class period for a structured lecture component. In addition to broadening the student's experience, it is prudent for instructors to have some presentation materials prepared in advance for common questions which arise on mathematically intensive subjects such as cryptanalysis, key wrapping, Diffie-Hellman, Rivest-Shamir-Adelman (RSA), and other common elements of the cybersecurity curriculum. Reviewing these concepts from a different point of view than the text book allows students the opportunity to reinforce the new concepts by making connections with other learning goals from related coursework in programming or math.

Another important aspect of cybersecurity education which lends itself to a hybrid approach is supplementing the class resources with recent examples of real world security breaches. Students in the Marist College program and at NYCCT are also given hands-on experience with lab tools such as FileZilla, WireShark, Metasploit, OpenVAS (with the GreenBone graphical user interface), Putty, NetWitness Investigator, Zenmap, and tftpd64. In a hybrid classroom, the instructor also guides the student to trusted learning resources covering recent cyber attacks (say, within the past three years). Students are cautioned to always refer back to a trusted reference such as the Common Vulnerabilities and Exposures (CVE), rather than gathering all their material from blogs or the popular media.

Understanding the implications of these attacks is facilitated by instructor-led discussion, which resembles a traditional lecture more than a flipped question and answer session. In the Marist Cybersecurity Curriculum, instructors heavily supplement learning resources with recent examples, often presenting

a “hack of the week” during classroom time. This reverses the traditional classroom flip, by presenting students with the framework of an attack and challenging them to relate this specific example to their understanding of basic security principles. Currently, at NYCCT, students are involved with the physical implementation of Local Area Networks (LANs) using off the shelf components. The implementation consists of three separate server-based LANS: Windows 2012 Server, Xen Server, and the VMware ESXi sever. Each server will interconnect to four or five clients running different Operating Systems (Windows 7, Windows 8, Kali Linux, Ubuntu, CentOS, etc.). Students experiment with several tools that are contained in the Kali Linux distribution. The physical LAN setup is in addition to the Virtual Laboratory that each student has already implemented to carry out their hacking skills in their own laptops for the flexibility of being a mobile laboratory.

For example, the instructor might assign learning resources from trusted sources discussing the many recent hacks on automobile computer systems as an introduction to security for the Internet of Things. These resources might include a discussion of the Control Area Network (CAN) and onboard diagnostics systems mandated by the federal government on all new vehicles since 1996. The instructor then leads a discussion about which basic security principles are violated by this design (for example, allowing low priority systems such as the air conditioning controller to access high priority systems such as the brakes is an access privileges issue, which leads to a discussion about least privileges, denial by default, and defense in depth). In the hybrid approach used at Marist College, students are also required to complete a semester-long case study of their own in which they must demonstrate how basic security principles may be applied to recent high profile attacks. The instructor’s lectures provide examples of this technique throughout the semester and attempt to teach students a constructive way of thinking when they approach security problems. Such a framework is critical in a rapidly changing field such as cybersecurity, where students will almost certainly encounter new hacking techniques and exploits throughout their careers. Instructor-led discussions on security fundamentals supplements independent student hands-on lab

experiences so that a student will be equipped to deal with new problems that don’t exactly match anything previously documented in the learning resources.

An effective hybrid approach requires careful preparation by the instructor and provides leading questions or supplemental materials which afford many opportunities to interact with the students. There are still useful opportunities for lecture presentations, but these are tempered with dynamic classroom environments in which the instructor and student explore new concepts together and the instructor suggests how these concepts may easily be incorporated into a student’s existing body of knowledge. While the roles of instructor and student are transformed from the conventional lecture hall approach, the transition is less dramatic (and thus less stressful) for the prepared student and instructor. Response to this approach has been overwhelmingly positive thus far, with the initial class offering in fall 2015 significantly exceeding enrollment expectations for a new course offering. Student feedback is continuously monitored throughout the semester, including anonymous polls of student satisfaction with pair programming techniques used in the labs. Students have also contributed technical research papers based on their coursework (Estrella et al. 2015; Cannistra et al. 2014). Future work in this area will investigate the application of predictive analytics to the student population in an effort to improve early detection of at-risk students.

## ACADEMIC AND INDUSTRY COLLABORATION

Cybersecurity is well suited to a hands-on, practitioner-oriented approach and benefits from a closer interaction between educators and the IT administrators at their institutions. More meaningful collaboration between different branches of academia, or between academia and industry, would also benefit students in this field. We have begun to explore collaborative opportunities in the region and plan to continue developing future efforts in this area.

Our collaboration extends to the emerging service industry perspective on networking and cybersecurity. Faced with a growing gap in practitioners with appropriate data center networking and security skills, the Institute for Service Industry Professionals (ISSIP)

has recently formed a series of working groups on topics such as the Internet of Things and Software Defined Networking (SDN). The mission of these groups includes promoting education, assessing the impact of new technologies on required knowledge and skill sets, and providing guidance to a consortium of academic and industry participants. These efforts respond to recent reports from computer industry analysis noting the lack of appropriate skills in these areas and the need for education reform in an industry where most of the networking-related jobs in 2014 did not exist just a few years ago (Sher-DeCusatis, DeCusatis, 2014). The flipped and hybrid flipped classroom approaches have implications for the network service industry and for network education and certification programs. Preparing for traditional network administrative and service roles involves complex, vendor-specific practitioner certification exams which rely on memorizing network device configuration commands and learning how to implement hop-by-hop distributed security. While these are valuable skills, the broader body of knowledge which benefits cybersecurity professionals has historically been de-emphasized for networking service practitioners. The flipped and hybrid flipped classroom approaches we are developing can be extended to include features of the rapidly evolving network landscape including SDN, Network Function Virtualization (NFV), and programmable application programming interfaces (APIs) on routers, firewalls, and long haul optical networking equipment. Indeed, the ability to program network infrastructure APIs is rapidly emerging as a key differentiating skill for radio network architects and administrators and will soon become a requirement for most employers.

Industry participation in the security curriculum has also been facilitated by recent statewide efforts to promote cloud computing as an economic growth engine. The capabilities and educational benefits of the CCAC have been described previously (Cannistra et al. 2014; Sher-DeCustatis et al. 2014). In keeping with their mission to promote the economic benefits of this technology across the state, Marist has formed academic partnerships with other public, private, and Ivy League schools, including NYCCT as well as industry partners including IBM, Brocade, Ciena, Adva, and many others. The collaboration between multiple industry sponsors and academic partners provides a force multiplier which increases the impact on a student's education and is based on the National

Science Foundation's Industry and University Cooperative Research Center (IU/CRC) model. By training students with cybersecurity principles that are of interest to the lab's corporate sponsors, this lab provides a very high placement rate for students after graduation. CUNY students have the opportunity to collaborate with the CCAC and take advantage of their facilities to further their interest in cloud security. Marist is also developing a series of courses which will lead to a degree specialization in cybersecurity, leveraging the capabilities of the CCAC lab and its academic partners. This nontraditional, federated approach to technical education has yielded many benefits for the institutions involved and provided students with a richer undergraduate experience. Students at each of the participating schools can take advantage of the test bed at Marist College to conduct undergraduate research projects or independent study as well as developing a bridge to graduate studies. Remote access to the Marist test bed is being enabled for wireless devices such as smart phones and tablet computers. The CCAC has an established record of undergraduate student contributions to open source software development projects, which are expected to benefit from an increased focus on cloud security. By making cybersecurity accessible in this way, we can provide a much richer experience for undergraduate students with basic programming skills and an interest in data networking.

## CONCLUSIONS AND FUTURE WORK

The industry-wide emphasis on cybersecurity and a recognized shortage of security professionals has driven a renewed focus on the cybersecurity education process. We have investigated a novel approach to cybersecurity education using variations on the flipped classroom model. This program appears to be particularly well suited to engaging nontraditional and under-represented students because of its practical, hands-on focus and engagement with other academic and industry partners. The curriculum does not require extensive prerequisites and can be deployed quickly at very low startup cost in an isolated, inherently secure student training environment. We have begun to make this technology accessible to a student population which includes a high percentage of under-represented students, enabling them to pursue

opportunities with leading financial companies and other employers. Undergraduate students are capable of making meaningful contributions to research in this area due to the emphasis on open source software and industry standard security protocols. In the future, we plan to produce more instructional materials and explore the use of predictive analytics to identify at-risk students.

## REFERENCES CITED

Association for Computing Machinery (ACM). (n.d.). *Toward curricular guidelines for cybersecurity*. Retrieved from <https://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf>

Bishop, J., Verleger, M. (2013, June 23-26). *The flipped classroom: a survey of research*. Address at 120th annual ASEE Conference and Exposition, Atlanta, GA.

Cannistra, R., Carle, B., Johnson, M., Kapadia, J., Meath, Z., Miller, M., Young, D., DeCusatis, C., Bundy, T., Zussman, G., Bergman, K., Carranza, A., Sher-DeCusatis, C., Pletch, A., Ransom, R. (2014). Enabling autonomic provisioning in SDN cloud networks with NFV service chaining. *Proceedings of OFC Annual Meeting*, San Francisco, CA.

Carranza, A., DeCusatis, C. (2015). Implementing a flipped classroom for cybersecurity education. *Proceedings of ASEE Northeast Annual Meeting*, Villanova University, Philadelphia, PA.

Carranza, H., Carranza, A. (2014). Cryptographic validity in network security. *Proceedings of IEEE Mid-Hudson Section Workshop on Advanced Technology for Next Generation Computing*, State University of New York, New Paltz, NY.

Cisco. (2014). Annual security report. Retrieved from [https://www.cisco.com/web/offer/gist\\_ty2\\_asset/Cisco\\_2014\\_ASR.pdf](https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf).

Corno A. (2014). Evolution of the network engineer job role. *Proceedings of SDN Workshop, 2014 Annual Meeting of the Association of Technology Management and Applied Engineering (ATMAE)*, St. Louis, MO.

Estrella, Y., Carranza, A., DeCusatis, C. (2015, July 29-31). Comparing performance of physical and virtual environment penetration testing using Kali Linux. *Proceedings of Latin American and Caribbean Consortium of Engineering Institutions (LACCEI) XIII Conference, paper 0422, p. 20-27*, Santo Domingo, Dominican Republic.

Exec. Order No. 13636 (2013, February). Retrieved from <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>

Florez, A., Piure, D., Carranza, A. (2014, November 6). Cloudstack and Openstack battle for network storage. *Proceedings of IEEE Mid-Hudson Section Workshop on Advanced Technology for Next Generation Computing*, State University of New York, New Paltz, NY.

IT Career Finder. (2014-15). Security jobs report. Retrieved from <http://www.itcareerfinder.com>

National Initiative for Cybersecurity Careers and Studies. (2015). Retrieved from <http://niccs.us-cert.gov/>

The National Initiative for Cybersecurity Education. (2015). Retrieved from <http://csrc.nist.gov/nice/index.htm>

Obama, B. (2015, February). Remarks by the President at the Cybersecurity and Consumer Protection Summit. Retrieved from <https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit>

Sams, A., Bergmann, J., Daniels, K., Bennet, B., Marshall, H., Arfstrom, K. (2014). What is flipped learning: the four pillars of f-l-i-p. Retrieved from [www.flippedlearning.org/cms/lib07/VA01923112/Centricity/Domain/46/FLIP\\_handout\\_FNL\\_Web.pdf](http://www.flippedlearning.org/cms/lib07/VA01923112/Centricity/Domain/46/FLIP_handout_FNL_Web.pdf)

Sher-DeCusatis, C., DeCusatis, C. (2014). Developing a software defined networking curriculum through industry partnership. *Proceedings of ASEE Annual Meeting*, Hartford, CT.

Presidential Policy Directive. (2015). Critical infrastructure security and resilience. Retrieved from <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>

White House. (2015). *The Comprehensive National Cybersecurity Initiative*. Retrieved from <https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>

Wilcox, L.C., Wilcox, M.S. (2013, April 26-28). A review and evaluation of engineering education in transition. *Proceedings of the IEEE 8th International Conference on Computer Science and Education (ICCSE)*, Sri Lanka.

Zafar, S., Carranza, A. (2014). Penetration testing using Kali Linux within VMware virtual networks. *Proceedings of the IEEE Mid-Hudson Section Workshop on Advanced Technology for Next Generation Computing*, State University of New York, New Paltz, NY.

## AUTHORS

**Aparicio Carranza** ([acarranza@citytech.cuny.edu](mailto:acarranza@citytech.cuny.edu)) is an associate professor in the Department of Computer Engineering Technology, New York City College of Technology (NYCCT), of the City University of New York (CUNY), Brooklyn, New York, and adjunct instructor at State University of New York (SUNY) at New Paltz. His research involves cybersecurity and technology education, Software Defined Networking (SDN), virtualization and cloud computing, and Linux clustering. He serves as an advisory council to four colleges (Vaughn College of Aeronautics and Technology, New York; DeVry University, New York; Technical Career Institute College of Technology, New York; and SUNY Rockland Community College) and was chair of his department from 2007 to 2013. Dr. Carranza earned a doctorate in electrical engineering from The Graduate School and University Center—CUNY; Bachelor of Science in

Electrical Engineering and Master of Science in Electrical Engineering from The City College of New York—CUNY; and an Associate of Applied Science in Electronics Circuits and Systems from Technical Career Institutes of New York. Dr. Carranza joined the Computer Engineering Technology Department of New York City College of Technology as full-time faculty in fall 2000. For several years he worked as an engineer and scientist at the Development Division of IBM Corporation in Poughkeepsie, New York. He teaches analog electronics, digital electronics, several programming languages (including MATLAB, C, C++, and Java, Python), engineering analysis, data communications, engineering design and other related courses.

**Casimer DeCusatis** ([Casimer.DeCusatis@marist.edu](mailto:Casimer.DeCusatis@marist.edu)) is an assistant professor in the Department of Computer Science and Mathematics, Marist College, Poughkeepsie, New York. His research with the New York State Cloud Computing and Analytics Center includes optical data networks, cybersecurity, and software-defined data centers. An IBM Distinguished Engineer Emeritus, he is also an IBM Master Inventor with over 150 patents and the recipient of several industry awards, including the Institute of Electrical and Electronics Engineers (IEEE) Kiyoo Tomiyasu Award, the Sigma Xi Walston Chubb Award for Innovation, the EDN Innovator of the Year Award, the Mensa Research Foundation Copper Black Award for Creative Achievement, the Penn State Outstanding Scholar Alumnus Award and Mark Luchinsky Memorial Lecture, and the IEEE/Eta Kappa Nu (HKN) Outstanding Young Electrical Engineer Award (including a citation from the President of the United States and an American flag flown in his honor over the United States Capitol). He is co-author of more than 200 technical papers, book chapters, and encyclopedia articles, a 2015 Cisco Distinguished Speaker, and editor of the *Handbook of Fiber Optic Data Communication* (now in its fourth edition). Dr. DeCusatis received his master's and doctoral degrees from Rensselaer Polytechnic Institute, (Troy, New York), in 1988 and 1990, respectively, and his bachelor's degree in the Engineering Science Honors

Program from the Pennsylvania State University (University Park), in 1986. He is a Fellow of the IEEE, Optical Society of America, and SPIE (the international optical engineering society), a member of the Order of the Engineer, Tau Beta Pi, Eta Kappa Nu, and various other professional organizations and honor societies.



# Malware Fingerprinting: Analysis of Tool Marks and Other Characteristics of Windows Malware

Sean McVey

## ABSTRACT

Trojans and other malware are common tools of cyber espionage. As such, it is useful to analyze attack malware for not only its method of operation but also for indicators of its origin. This paper will introduce the reader to techniques useful in the attribution or attempted attribution of Windows malware to its author or authors. Malware families will be discussed, as will the analysis of strings, Dynamic Link Libraries (DLLs), and language indicators. Analysis of command and control (C2) schemes will also be covered.

Independent of who is doing the research, malware analysis comes down to looking for tool marks (the information left behind in the process of creating malware), analysis of code behavior, and analysis of the overall modes of action of the code. These three areas can indicate relationships between distinct pieces of code, and can point to an individual author or threat group. This paper will discuss the types of information found in malware that can be useful in attribution.

## METHODS OF MALWARE ANALYSIS

Malware analysis can be broken down into two broad categories: static analysis and dynamic analysis. Static analysis involves “examining and analyzing the contents of the file without launching it” while dynamic analysis involves “loading the file onto a testbed system [virtual machine or otherwise] and launching it, while monitoring it to determine what effects it has on the system” (Carvey, 2005). Static and dynamic analysis can be further broken down into basic and advanced techniques as described below.

### Static Analysis

#### ■ Basic Static Analysis

Basic static analysis consists of examining the executable file [for human readable strings of text] without viewing the actual [code] instructions. Basic static analysis can confirm whether a file is malicious, provide information about its functionality ... basic static analysis is straightforward and can be quick, but it's largely ineffective against sophisticated malware, and it can miss important behaviors (Sikorski & Honig, 2012).

## INTRODUCTION

Much has been published about the detection of malware and the function of different types of malware but little has been published on malware attribution. This said, malware attribution, which is the process of identifying the malware author, is commonly conducted by researchers and analysts in academic, private, and government organizations. Attribution is critical in stopping bad actors (criminal and nation state) and can serve as a possible deterrent to other would-be attackers. Unfortunately, attribution can be elusive, and even the best attempts can fail or worse misattribute an attack. Because of this uncertainty, many researchers stop short of providing attribution outright. Instead, they hint at a source or provide useful clues that allow the reader to draw their own conclusions.

### ■ Advanced Static Analysis

Advanced static analysis consists of reverse-engineering the malware's internals by loading the executable into a disassembler and looking at the program instructions in order to discover what the program does. The instructions are executed by the CPU, so advanced static analysis tells you exactly what the program does. However, advanced static analysis has a steeper learning curve than basic static analysis and requires specialized knowledge of disassembly, code constructs, and Windows operating system concepts (Sikorski & Honig, 2012).

## Dynamic Analysis

### ■ Basic Dynamic Analysis

Basic dynamic analysis techniques involve running the malware and observing its behavior on the system in order to remove the infection, produce effective signatures, or both ... Like basic static analysis techniques, basic dynamic analysis techniques can be used by most people without deep programming knowledge, but they won't be effective with all malware and can miss important functionality (Sikorski & Honig, 2012).

### ■ Advanced Dynamic Analysis

Advanced dynamic analysis uses a debugger to examine the internal state of a running malicious executable. [Using] advanced dynamic analysis techniques provide another way to extract detailed information from an executable. These techniques are most useful when you're trying to obtain information that is difficult to gather with the other techniques (Sikorski & Honig, 2012).

Within these four categories, there is a wide range of analysis approaches, from monitoring the changes made by the malware code to analysis of the malware code itself. Code analysis, such as disassembly of the code to its assembly language, "a programming

language that is one step away from machine language", is considered the most complex technique (PC Magazine, n.d.). Advanced techniques provide the most detailed picture of the capabilities and function of the malware code but they take more skill and time to do correctly. On the other hand, websites such as Virustotal.com and Anubis can offer the average user a quick analysis of malware code, but may not catch everything. In order to gain a complete picture of the malware (the behavior, mode of action, author's style, and tool marks), it's likely that more than one technique will be needed. Although, basic static analysis such as the examination of strings (human readable text found in the code) may at times hold the smoking gun.

## TOOL MARKS AND THE AUTHOR'S SIGNATURE

In traditional forensics, *tool marks* are defined as "features imparted on an object by the contact and force exerted from a tool" (Hernandez, 2011). In malware analysis, tool marks refers to data found in the code, which not only indicate how the code was created, but when it was created and much more. Tool marks can include file names and paths, compiler specific information, and other data intentionally and unintentionally left behind in the code. Tool marks can be thought to fall into three categories: tool marks related to format and structure of the code itself, tool marks related to creation and debugging of the code, and finally, tool marks related to programmer chosen values. This last category—programmer chosen values—includes file names, registry keys, "shout-outs" to other hackers, and other style choices. These programmer specific choices can be considered the signature of the author. Common tool marks are listed in Table 1 below.

TABLE 1: USEFUL TOOL MARKS

TOOL MARK TYPE	SOURCE
BUILD DATE	PE Data
BUILD VERSION	PE Data
CHARACTER SET (LANGUAGE)	PE Data
CODE STYLE	Author
COMMENTS	PE Data
FILE AND FOLDER NAMES	Author
FUNCTION CALL (SYMBOL) USE	Code & Author
LANGUAGE CODE	PE Data
MUTEX VALUE	Author
NAME MANGLING	Code
PACKING	PE Data
PROGRAM DATABASE (PDB) BUILD PATH	Code & Author
REGISTRY KEY NAMES	Author
RICH SIGNATURE	Code
SERVICE NAMES	Author
UNIQUE STRINGS	Author

In Windows systems, the format used for executable files is known as the Portable Executable (PE) format (Pietrek, 2002). These PE files are structured and contain both the executable code, as well as metadata about the code itself. PE metadata can include a range of information such as the date the file was created, the date the code was compiled, version information (some malware authors track code versions), comments, file packing, and information about the language settings of the system it was compiled on (Microsoft, 2013). For example, an analysis of the PE information of Memory Monitor, an earlier version of the malware used in the Target data breach, indicates that it was written using Russian language settings and was created in March of 2013. Figure 1 includes a representation of Memory Monitor’s PE information.

FIGURE 1:  
MEMORY MONITOR PORTABLE  
EXECUTABLE (PE) INFORMATION

```

$ sudo exiftool -s 22DAF.exe
ExifToolVersion : 9.51
FileName : ██████████\22DAF.exe
Directory : ██████████
FileSize : 382 KB
FileModifyDate : 2014:01:16 19:39:48-05:00
FileAccessDate : 2014:02:16 12:25:24-05:00
FileNodeChangeDate : 2014:02:16 12:25:24-05:00
FilePermissions : rwxr-xr-x
FileType : Win32 EXE
MIMEType : application/octet-stream
MachineType : Intel 386 or later, and compatibles
TimeStamp : 2013:03:23 06:18:42-04:00
PEType : PE32
LinkerVersion : 5.0
CodeSize : 303184
InitializedDataSize : 8192
UninitializedDataSize : 543760
EntryPoint : 0xc9900
OSVersion : 4.0
ImageVersion : 0.0
SubsystemVersion : 4.0
Subsystem : Windows GUI
FileVersionNumber : 1.3.2.7
ProductVersionNumber : 1.3.2.7
FileFlags : 0x003f
FileOS : (none)
FileOS : Win32
ObjectFileType : Executable application
FileSubtype : 0
LanguageCode : Russian
CharacterSet : Windows, Cyrillic
CompanyName : Microsoft
FileDescription : drivers
FileVersion : 1.3.2.7
InternalName : Microsoft
LegalCopyright : Windows
LegalTrademarks : Windows
OriginalFilename : Microsoft help
ProductName : Microsoft help
ProductVersion : 1.0.0.0
Comments : ██████████
  
```

Notice in Figure 1, the company name and copyright information have been set by the malware author to Microsoft in an effort to make the program seem legitimate.

PE files created using Microsoft’s Visual Studio programming environment contain a signature that can be used to track a piece of code to a given machine. The rich signature is not part of the PE metadata; instead it is placed in the executable when it is compiled. The Rich Signature does not contain personally indefinable information per se, but does contain “compiler id’s which are gathered by the linker” and “contain[s] the

version number of the compiler” itself (“Things They Didn’t Tell You,” 2004). While the long-term stability of this signature is questionable, it serves as distinct signature of the machine used to compile the code. Memory Monitor’s rich signature as decoded by Daniel Pistelli’s PE Insider tool is depicted in Figure 2.

FIGURE 2: MEMORY MONITOR RICH SIGNATURE

```

1 ; Rich Signature
2
3 product id: 0x0083 minor build version: 30729 count: 2
4 product id: 0x0098 minor build version: 20115 count: 11
5 product id: 0x009E minor build version: 30319 count: 14
6 product id: 0x009C minor build version: 30319 count: 8
7 product id: 0x0093 minor build version: 30729 count: 11
8 product id: 0x0001 minor build version: 0 count: 2695
9 product id: 0x00AA minor build version: 30319 count: 64
10 product id: 0x00AB minor build version: 30319 count: 296
11 product id: 0x009B minor build version: 30319 count: 1
12 product id: 0x009A minor build version: 30319 count: 1
13 product id: 0x009D minor build version: 30319 count: 1

```

Depending on the programming language the code is written in, variable names and other text may be put through a process called “name mangling” as part of the compiling process. Name mangling helps to avoid

(Kefallonitis, 2007). Because each compiler mangles names differently yet predictably, analysis of the code can indicate the language the code was written in and the type of compiler used—useful information when profiling a programmer. Examining symbols and the Dynamic Link Libraries (DLL) used can further create a picture of the programmer’s environment. Usage of specific DLLs can indicate the version of Visual Studio (Figure 3) or other development environments used to create the code.

Program database (PDB) files were introduced along with Visual C++ version 1.0 to hold debug information for programs written in Visual Studio (Microsoft, 2005). PDB paths are tool marks left over from the debugging process in Visual Studio. PDB paths won’t exist in release code or code not written in Visual Studio. When found these paths point to the location of the code on the malware writer’s system at the time it was compiled. Analysis of PDB paths is common because the uniqueness of these paths serve as a good fingerprint and can indicate the programmer’s name for the malware. At times the PDB path can indicate the nature of the malware itself. Analysis

FIGURE 3: MICROSOFT VISUAL C++ DLLS BY VERSION (MICROSOFT, 2008)

DLLS USED IN VISUAL C++ 5.0	DLLS USED IN VISUAL C++ 6.0	DLLS USED IN VISUAL C++ .NET 2002	DLLS USED IN VISUAL C++ .NET 2003	DLLS USED IN VISUAL C++ 2005	DLLS USED IN VISUAL C++ 2008
MSVCRT.DLL	MSVCRT.DLL	MSVCR70.DLL	MSVCR71.DLL	MSVCR80.DLL	MSVCR90.DLL
MSVCRTD.DLL	MSVCRTD.DLL	MSVCR70D.DLL	MSVCR71D.DLL	MSVCR80D.DLL	MSVCR90D.DLL
MSVCP50.DLL	MSVCP60.DLL	MSVCP70.DLL	MSVCP71.DLL	MSVCP80.DLL	MSVCP90.DLL
MSVCP50D.DLL	MSVCP60D.DLL	MSVCP70D.DLL	MSVCP71D.DLL	MSVCP80D.DLL	MSVCP90D.DLL
MSVCIRT.DLL	MSVCIRT.DLL				
MSVCIRTD.DLL	MSVCIRTD.DLL				

“name collisions, [and allows for] name overloading, and type checking” (IECC.com, 1999). Name mangling can be used for security through obscurity and is an important aspect of code obfuscators. Name mangling is also highly “compiler dependent”

of the Memory Monitor code (Figure 4) finds that at the time it was compiled its author had it saved as *mmon* in *x:\Programming\C++\2011.08\ScanMemory\Debug*. In this case, “Scan Memory” is a clue to its intended function.

FIGURE 4: PDB PROJECT PATH

```
004BA9E8 ASCII: x:\Programming\C++ 2011.08\ScanMemory\De...
004BA9E8 : 78 3A 5C 50 72 6F 67 72 61 6D 6D 69 6E 67 5C 43 x:\Programming\C
004BA9F8 : 2B 2B 20 32 30 31 31 2E 30 38 5C 53 63 61 6E 4D ++ 2011.08\ScanM
004BAA08 : 65 6D 6F 72 79 5C 44 65 62 75 67 5C 6D 6D 6F 6E emory\Debug\mmon
004BAA18 : 2E 70 64 62 00 00 00 00 E0 C0 43 00 00 .pdb.....C..
```

Mutual Exclusion, or Mutex, values are a common way to identify code. Mutex values are a normal part of many applications that serve to prevent “simultaneous access to a shared resource” by running code (Janssen, n.d.). Sometimes referred to as mutants, malware uses Mutex values to manage process threads and prevent re-infecting a machine. Mutex values are meant to be unique by design and are set by the programmer; because of this they can tie versions of malware together into a family if consistently used. Mutex values have also been used to attribute malware back to a particular author when reused in attributable code (Hoglund, 2010).

How the malware itself is written can be used to profile the programmer. Use of legacy or outdated system and function calls can, for example, hint at the age and experience of a programmer (Spafford & Weeber, 1992, p. 7). The overall structure, complexity, and stability—for example, are there bugs?—of the malware can indicate the knowledge and experience of the malware author as well (Spafford & Weeber, 1992). Filenames, Registry key names, service names, as well as arbitrary values such as sleep times and other unique constants may all serve to create a fingerprint. If analyzed correctly, strings of almost any type could

possibly be used to weave malware into families and connect author to attributed code. Analysis of the Memory Monitor malware uncovers a number of strings, including a Registry key and application name (Figure 5). Both are useful in detection and attribution.

FIGURE 5: MEMORY MONITOR REGISTRY KEY AND SERVICE NAME

```
REG ADD HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v
videodrv /t REG_SZ /d " - Module: svhst.exe, Process: svhst.exe, Offset:
0007132F

The string 'REG ADD
HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v
videodrv /t REG_SZ /d "' was found in the module 'svhst.exe'. This is a
regkey used to survive reboot. The string was found at offset 0007132F from the
start of the module.
```

Malware writers will often times try to obfuscate and prevent analysis of their code. The way in which malware code is obfuscated along with the presence of other anti-forensic techniques may be particular to a specific programmer when taken together, and the complexity of the protection may speak to the knowledge and skill of the programmer. Some common obfuscation and anti-forensic techniques are captured in Figure 6.

FIGURE 6: OBFUSCATION AND ANTI-FORENSICS TECHNIQUES

NAME	DESCRIPTION	TYPE
ANTI-DISASSEMBLY & DEBUGGING	Techniques used to slow or prevent analysis of the code	Anti-forensic
BASE64 ENCODING	Represents binary data using upper and lowercase letters as well as numbers	Obfuscation
PACKING	Compression used to obscure the code	Obfuscation
VITALIZATION DETECTION	Detects when the code is operating in a virtual machine	Anti-forensic
XOR	Simple binary operation that uses a set key to Obscure the data	Obfuscation

Tool marks vary in complexity. Some may only be visible using advanced techniques while others such as file paths, symbol names, and PDB paths may be visible using basic static analysis. While we have covered some common tool marks there are many more not mentioned here. By using these tool marks and others found through static and dynamic analysis the attribution process can begin.

## CODE BEHAVIOR






The behavior of malware, what it does, what it's after, and its complexity are factors that should be taken into account as part of the attribution process. Information stealing malware, for example, is likely to have a different motive behind it than a banking trojan or adware and the likely motives should be taken into account when building an overall picture of the attacker.

Analysis of the complexity of malware code, as well as the knowledge needed for it to operate, is also a useful point of analysis. A good example of this is the Stuxnet malware, which exploited “four 0-day vulnerabilities, compromise[d] two digital certificates, and inject[ed] code into industrial control systems and [hid] the code from the operator” (Falliere, Murchu, & Chien, 2011, p. 55). Stuxnet is a highly complex, targeted threat designed to attack a specific target, likely in Iran (Falliere, Murchu, & Chien, 2011, p. 2). The complexity, behavior, and targeted nature of the Stuxnet malware make it likely that the group behind it had access to intelligence and a wide range of technical resources. Such a profile indicates that Stuxnet was created by a state or state-funded group rather than a lone hacker or cybercrime group. In contrast, malware such as Memory Monitor is designed to steal credit card information, and while budget deficits might loom large it is likely that a cyber criminal or gang—not a nation state—is behind it.

Malware can also be examined to reveal individual behaviors of the code. Examination of behavioral traits instead of signatures often identifies suspicious code even if it had not previously been identified, as in the case of 0-day threats. Analysis of our example

malware with Responder Pro, a malware analysis tool, shows a number of suspicious traits including reading the memory space of other processes and possible keystroke interception (Figure 7). Automated tools greatly aid in analysis of behavioral traits but are not necessary.

FIGURE 7: SAMPLE OF MEMORY MONITOR CODE TRAITS

	<b>Trait:</b> 06 BC
	<b>Description:</b> Program is walking the list of open windows. It may be looking for a specific window so that it can interact with it.
	<b>Trait:</b> 47 22
	<b>Description:</b> Program is searching the filesystem for files.
	<b>Trait:</b> 1B 2A
	<b>Description:</b> Program is reading the memory of another process. This is not typical to most programs and is usually only found in system utilities, debuggers, and hacking utilities.
	<b>Trait:</b> 4C 5D
	<b>Description:</b> A method for intercepting keystrokes from the data path that relies on an event, callback, or signal being delivered to the sniffing program. This is not suspicious by itself and is used by many GUI based apps on windows.
	<b>Trait:</b> 6F E1
	<b>Description:</b> Program appears to replace the default blocking hook function in the sockets library. This is an obscure design factor that the developer used when building the software.

## MODE OF ACTION

The last area of examination when attempting attribution is analysis of the way the malware infects its target, communicates with the outside world, and otherwise operates. Methods of delivery, exploitation, and command and control (C2) differ widely from malware to malware but may be similar between malware in the same family or even the same threat group.

### Delivery

Malware can be delivered to its victim in a number of ways. Seemingly harmless files can be infected with malware to create trojans waiting to be downloaded off the web, while others may take advantage of an infected web server to propagate malware code. Delivery of the malware need not be complex

in order to be effective. Analysis of major advanced persistent threat (APT) campaigns, including APT1 (Mandiant, 2013), Lurid Downloader (Villeneuve & Sancho, 2011), and GhostNet (Information Warfare Monitor, 2009) illustrate that sending targeted e-mails (spear-phishing) is a favorite technique of APT actors. Analysis of the delivery method, including related spear-phishing e-mails or trojanized files, provide valuable clues about the source and nature of the attack.

## Exploitation

Short of the victim being tricked or “social-engineered” into running malware code, malware often exploits a weakness in the operating system or commonly used application such as web browsers and PDF viewers in order to infect a system. The exploit or exploits used can be a point of attribution. As noted earlier, Stuxnet exploited not one but four 0-day, i.e. previously unknown, vulnerabilities. Again, this speaks to the skill and resources of the Stuxnet authors. The application exploited can also provide clues to both the target and likely source of an attack. Malware targeting an application popular in a given region or with a group, such as QQ chat popular in China, may hint at groups interested in targeting that population (P. Breuer, personal communication, February 21, 2014).

## Command and Control

Understanding how malware communicates to the outside world is a critical factor in malware attribution. IP addresses and domain names may be obscured but when identified they can point to command and control (C2) servers and a responsible party. Further, threat actors may reuse the same “infrastructure” of servers and hop-points, therefore identifying the C2 system may speed attribution (P. Breuer, personal communication, February 21, 2014). Analysis of malware C2 systems can tell researchers not only about the threat actor, but can also help identify victims. Analysis of the command and control system of the Koobface malware allowed researchers to understand how the

botnet worked and even identify payments made to people involved (Villeneuve, 2010). As illustrated in Figure 8 and Figure 9, in analyzing our sample malware, a much simpler line of communication is identified. An IP address (109.234.159.254) as well as a Web address (ree3.7ci.ru) are easily found.

FIGURE 8: IP ADDRESS FOUND IN MEMORY MONITOR

**Found IP: 109.234.159.254 - Module: svhst.exe, Process: svhst.exe, Offset: 000711A3**

The package 'svhst.exe' contains a dotted decimal string: 109.234.159.254. Review this to determine if an IP address has been found. This match was found at offset 000711A3 from the start of the module.

FIGURE 9: WEB ADDRESS FOUND IN MEMORY MONITOR

**www.ree4.7ci.ru/reports/readme.txt - Module: svhst.exe, Process: svhst.exe, Offset: 000712DD**

The string 'www.ree4.7ci.ru/reports/readme.txt' was found in the module 'svhst.exe'. This is a potential txt file. The string was found at offset 000712DD from the start of the module.

## ANALYSIS AND ATTRIBUTION

Once the tool marks, code behaviors, and mode of action are collected, a fingerprint of its author becomes apparent. Once gathered, open-source intelligence (OSINT) research can begin. Code repositories, hacker forums, and other websites can be searched for unique data found in the code. Analysis of the malware’s C2 structure can identify servers and communication methods, which in turn may reveal additional clues to the attacker’s identity.

With this in mind let’s take a look at the details of our example malware to see what we have learned in Figure 10.

FIGURE 10: COLLECTED TOOL MARK AND C2 INFORMATION

TYPE	VALUE
MALWARE NAME	Memory monitor
SERVICE CREATED	svhst.exe
METHOD OF PERSISTENCE	Registry Key
REGISTRY KEY DETAIL	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\videodrv
PROJECT PATH	x:\Programming\C++ 2011.08\ScanMemory\Debug\mmon.pdb
CREATION DATE	3/23/13 6:18
VERSION	1.3.2.7
LANGUAGE CODE	Russian
CHARACTER SET	Windows, Cyrillic
WEB ADDRESS	ree4.7ci.ru
IP ADDRESS	109.234.159.254

In this instance the method of infection for Memory Monitor is unknown. It was likely copied onto the target system by the attacker since Memory Monitor is not known to be viral or use an exploit to infect its target. In reviewing the information gathered in Figure 10, it is clear that the code was likely written by a Russian speaker on a Windows system set to use Cyrillic. Analyses of the IP address tracks back to a Russian ISP as well, and is described in Figure 11.

Memory Monitor is related to the malware used in the Target stores breach in late 2013. As a fairly well known piece of malware, much has been written about it and its author making attribution unusually easy. It is also a fairly simple piece of code with distinct strings and few anti-forensic features. In reality attribution isn't usually this simple. Many hours of static and dynamic analysis may be needed to find useful tool marks and puzzle out how the malware functions.

FIGURE 11: IP ADDRESS INFORMATION

```
inetnum:        109.234.156.0 - 109.234.159.255
netname:        SELECTEL-NET
descr:          Selectel Ltd.
country:        RU
admin-c:        AKME
tech-c:         AKME
status:         ASSIGNED PA
mnt-by:         MNT-SELECTEL
source:         RIPE # Filtered

person:         Akhmetov Vyacheslav
address:        191015, Russia, Saint-Petersburg, ul. Tverskaya, d 8 liter B
mnt-by:         MNT-SELECTEL
phone:          +78127188036
nic-hdl:        AKME
source:         RIPE # Filtered

route:          109.234.159.0/24
descr:          Selectel Moscow Data-center
origin:         AS49505
mnt-by:         MNT-SELECTEL
source:         RIPE # Filtered
```

Analysis of the web address “ree4.7ci.ru” leads to further information about the malware writer himself, reported to be a Russian 17-year-old with ties to cyber criminals. Attribution achieved.

## CONCLUSION

It must be said that it is almost impossible to know with 100% certainty who is really behind an attack using just malware analysis. Malware code can be stolen, accounts hijacked, and tool marks can be faked—there is always the possibility of deliberate misdirection and misattribution. That said, author attribution is possible. By building a careful chain of evidence out of tool marks and other malware attributes, it is possible to link malware to its source within a reasonable amount of certainty. Where possible, other intelligence gathering methods such as signals intelligence (SIGINT) and even human intelligence (HUMINT) can add precision and certainty to attribution.



## REFERENCES CITED

- Carvey, H. (2005). Malware analysis for windows administrators. Digital Investigation, 19-22.
- Falliere, N., Murchu, L. O., & Chien, E. (2011). W32.Stuxnet Dossier. Symantec Security Response. Symantec.
- Harvey, P. (2011, July 12). *EXE Tags*. Retrieved from <http://www.sno.phy.queensu.ca/~phil/exiftool/TagNames/EXE.html>
- Hernandez, G. A. (2011, September 23). *Firearms, Tool Marks, and Other Impressions—Keynote\_Hernandez.pdf*. Retrieved from [http://www.dtic.mil/ndia/2011ballistics/Keynote\\_Hernandez.pdf](http://www.dtic.mil/ndia/2011ballistics/Keynote_Hernandez.pdf)
- Hoglund, G. (2010). Malware Attribution: Tracking Cyber Spies & Digital Criminals. *Blackhat Vegas 2010*. Las Vegas, NV: Blackhat.
- IECC.com. (1999, June 30). *Symbol management*. Retrieved from <http://www.iecc.com/linker/linker05.html>.
- Information Warfare Monitor. (2009). *Tracking GhostNet*. The Munk Centre for International Studies. Toronto: Information Warfar Monitor.
- Janssen, C. (n.d.). What is Mutual Exclusion (Mutex)? [Definition]. *Techopedia*. Retrieved from <http://www.techopedia.com/definition/25629/mutual-exclusion-mutex>.
- Kefallonitis, F. (2007, October 29). *Name Mangling Demystified*. Retrieved from [http://www.int0x80.gr/papers/name\\_mangling.pdf](http://www.int0x80.gr/papers/name_mangling.pdf).
- Mandiant. (2013). *APT1: Exposing One of China's Cyber Espionage Units*. Retrieved from <http://intelreport.mandiant.com/>.
- Microsoft. (2005, August 5). *Description of the .PDB files and of the .DBG files*. Retrieved from <http://support.microsoft.com/kb/121366>.
- Microsoft. (2008, March 19). *Description of the default C and C++ libraries ...* Retrieved from support.microsoft.com: <http://support.microsoft.com/kb/154753>.
- Microsoft. (2013, February 6). *Microsoft PE and COFF Specification*. Retrieved from <http://msdn.microsoft.com/library/windows/hardware/gg463125>.
- PC Magazine. (n.d.). Assembly Language [Definition]. *PC Magazine Encyclopedia*. Retrieved from <http://www.pcmag.com/encyclopedia/term/38047/assembly-language>.
- Pietrek, M. (2002, February). Inside Windows: An in-depth look into the Win32 portable executable file format. *MSDN Magazine*. Retrieved <http://msdn.microsoft.com/en-us/magazine/cc301805.aspx>.
- Pistelli, D. (2010, November 11). *Microsoft's Rich Signature*. Retrieved from ntc core.com: <http://ntcore.com/Files/richsign.htm>.
- Sikorski, M., & Honig, A. (2012). *Practical malware analysis*. San Francisco: No Starch Press.
- Spafford, E. H., & Weeber, S. A. (1992). *Software forensics: Can we track code to its authors?* Purdue University, Department of Computer Science. West Lafayette: Purdue University.

Things they didn't tell you about ms link and the pe header. (2004, July 7). Retrieved from <http://spth.virii.lu/29a8/Articles/29A-8.009.txt>.

Villeneuve, N. (2010). *Koobface: Inside a crimeware network*. Infowar Monitor, Munk School of Global Affairs. Infowar Monitor.

Villeneuve, N., & Sancho, D. (2011). *The "Lurid" Downloader*. TrendLabs. Trend Micro.

## AUTHORS

**Sean B. McVey** ([sean@everyday-data.com](mailto:sean@everyday-data.com)), EnCE, CISSP, is a Maryland-based incident response team lead and forensics subject matter expert at cybersecurity firm Antietam Technologies. Currently contracted to the U.S. Department of Energy, Mr. McVey is also a former instructor at the Defense Cyber Investigations Training Academy (DCITA) where he researched mobile device and Macintosh forensics. With over 10 years in the field of digital forensics, he holds a Master of Science in cybersecurity from Utica College and a Bachelor of Science in information technology from the Rochester Institute of Technology.



# Strengthening Cyber Incident Response Capabilities Through Education and Training in the Incident Command System

Austen D. Givens

## ABSTRACT

Supervisory Control and Data Acquisition (SCADA) systems control innumerable industrial processes that affect large segments of U.S. critical infrastructure, from regulating the flow of water through dams to calibrating the electrical currents in power substations located in residential neighborhoods. Historical evidence demonstrates that electronic attacks on SCADA systems can physically damage them. This can trigger consequences that must be simultaneously addressed by Computer Security Incident Response Teams (CSIRTs) and traditional first responders. This article advances a two-part argument: first, that the Incident Command System (ICS) offers a compelling means to strengthen cyber incident responses by integrating CSIRTs and first responders involved in SCADA incidents into a cohesive organizational structure; and second, that cybersecurity curricula in academic and professional training settings should therefore incorporate ICS education in order to increase the probability of effective incident responses involving CSIRTs and first responders in the future.

## Introduction

An oil pipeline running through central Siberia exploded one night in October 1982, sending an enormous fireball into the sky (National Security Archive, 2013). The blast was so powerful that it released the energy equivalent to that of a small atomic bomb (National Security Archive, 2013). The Central Intelligence Agency (CIA), in what may be the world's first-ever example of cyber sabotage, made the pipeline explode by introducing flawed computer code into the pipeline's control system, causing its components to malfunction (National Security Archive, 2013). This attack took advantage of electronic vulnerabilities in the pipeline's Supervisory Control and Data Acquisition (SCADA) systems, which regulated the movement of turbines in the pipeline that kept oil flowing from one point to another (National Security Archive, 2013). The CIA was able to exploit these vulnerabilities with the flawed computer code, causing the SCADA system to malfunction, ultimately resulting in the pipeline explosion.

Twenty eight years after the Siberian pipeline explosion, the U.S. government again used flawed computer code to damage physical infrastructure—this time, in Iran. In June 2010 Iranian nuclear officials discovered that many of the centrifuges that they were using to purify uranium had been badly damaged (Fildes, 2010). The U.S. and Israeli governments, which believed that Iran was using the uranium to build nuclear weapons, co-wrote and introduced a virus called Stuxnet into the centrifuge control systems (Fildes, 2010; Ferran & Radia, 2013). This highly sophisticated computer virus caused the centrifuges deliberately to spin out of control, breaking them (Fildes, 2010). The damage

was so widespread that one expert speculated that Stuxnet set back the progress of the Iranian nuclear program by two years (Katz, 2010). The Iranian government, however, denied that the damage had any serious impact on its nuclear ambitions (Warrick, 2011). Outside analysis by the Royal United Services Institute, a London-based defense think tank, confirms that Stuxnet's true long-term impact on the Iranian nuclear program was negligible (Barzashka, 2010, pp. 52–54).

The Siberian pipeline explosion and the Stuxnet virus demonstrate that attacks on SCADA systems can be used to cause physical damage to infrastructure. The risk of this type of damage is of increasing concern to U.S. federal officials. The Department of Homeland Security (DHS) recently ran a worldwide exercise to test response coordination to just such an incident (DHS, 2014). The need to prepare for physical infrastructure damage caused by SCADA system attacks gives rise to a fundamental question about cyber incident response capabilities in the United States: how are computer security experts, tasked with responding to the virtual effects of cyber attacks, and traditional first responders, who attend to the physical consequences of these incidents, to integrate their actions effectively?

This article argues that the Incident Command System (ICS), which has for years been used to manage conventional disasters, provides a ready-made and effective organizational structure for computer security experts and traditional first responders to integrate their responses to SCADA system attacks. Moreover, this article makes the case that since ICS can be used to blend the response actions of computer security experts and first responders, ICS training should be an integral part of cybersecurity curricula, precisely because of the rising need for computer experts and first responders to work closely with one another.

The rest of the article proceeds as follows. Part two briefly introduces ICS and frames the contribution of this study within the literature on ICS. Part three shows how ICS can effectively integrate cybersecurity experts and first responders into a single incident response framework. Part four makes the case that educational institutions and professional certification organizations should make ICS a central

component of their cybersecurity curricula. The article concludes by synthesizing the key themes presented in this analysis and offers recommendations for future research in this area.

## THE INCIDENT COMMAND SYSTEM (ICS)—AN OVERVIEW

ICS is a method, or way, to respond to emergencies. It superimposes an organizational coordinating structure on the uncertain and ever-changing conditions of an incident. Superimposing this management structure on the incident response permits one or more organizations to work together in a more streamlined, effective fashion. Moreover, ICS has been used successfully for at least 30 years, demonstrating that it is a viable way to manage emergency responses of any size or scope.

After the 9/11 terrorist attacks, ICS became a central focus of federal efforts to streamline and enhance incident response coordination. This renewed focus on ICS was in part a direct reaction to many of the coordination failures observed on 9/11, such as poor communication and collaboration among local government agencies in Manhattan following the collapse of the World Trade Center Twin Towers (9/11 Commission, 2004, pp. 319–322). Calls for a national standard in incident management led to the development of the National Incident Management System (NIMS) in 2004 (DHS, 2003; 9/11 Commission, 2004, p. 397).

Today NIMS is a national approach to incident management that covers all jurisdictions and functional areas (DHS, 2008). ICS is a central focus of NIMS (DHS, 2008b, pp. 45–63). In recent, notable large-scale incidents in the United States, public safety officials used ICS in response to Hurricane Katrina in 2005 and the powerful Joplin, Missouri tornado of 2011 (9/11 Commission, 2004; C-SPAN, 2011; DeAtley, 2011, pp. 12–13). Government agencies also use ICS throughout the United States on more routine, everyday emergencies, from house fires to hostage standoffs. And most recently, in the 2010 draft National Cyber Incident Response Plan (NCIRP), the U.S. Department of Homeland Security (DHS) identifies ICS as the response methodology of choice for managing significant cyber incidents (DHS, 2010, p. 16).

Figure 1 below depicts a prototypical ICS organizational structure. While detailed explanations of the specific positions shown in this ICS structure are beyond the scope of this article, what is noteworthy—and applicable directly to the management of SCADA incidents—is that ICS incorporates a diversity of actors performing distinct and complementary functions in the context of an incident response effort.

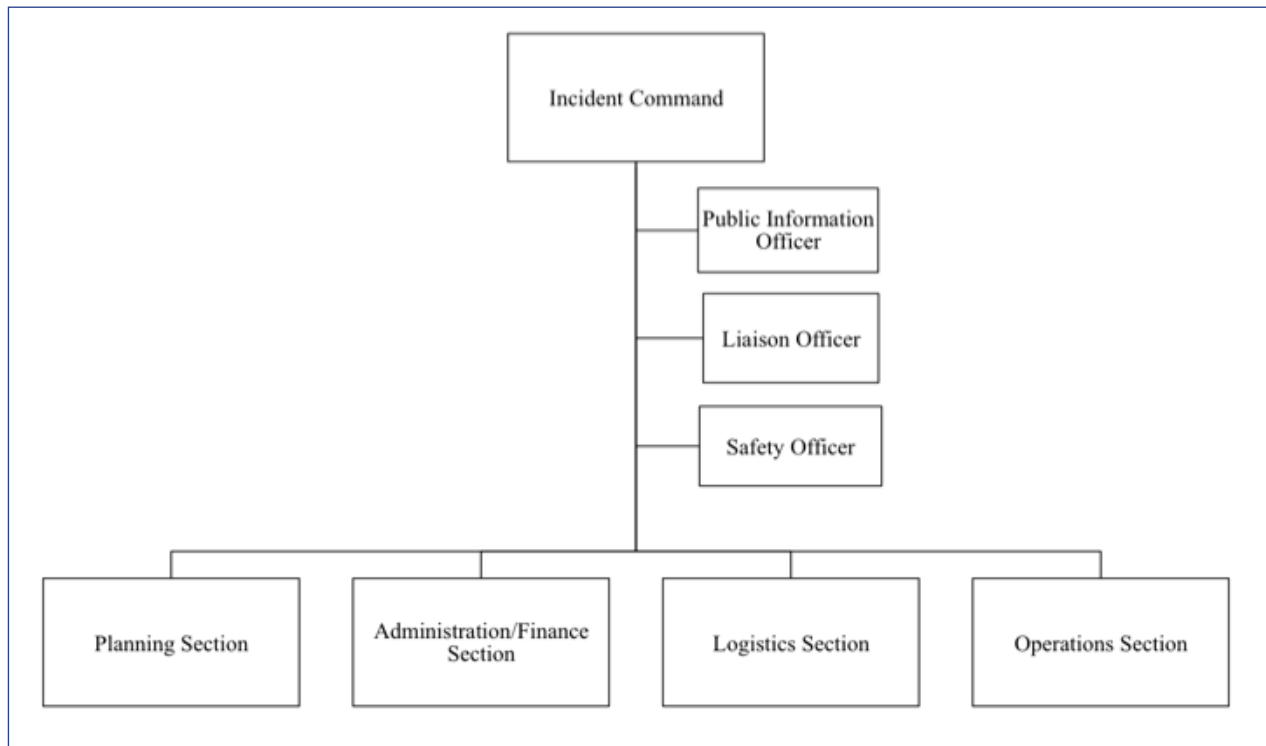
The Siberian pipeline explosion and Stuxnet examples introduced at the beginning of this article demonstrate that cyber incidents can have real-world consequences for the operation of critical infrastructure, particularly in the realm of SCADA systems. SCADA incidents can therefore require a coordinated response effort among computer security incident response teams (CSIRTs), which are specialized groups of information technology (IT) professionals that manage cyber incidents, and traditional first responders, like police officers, firefighters, and EMTs. This confluence of factors suggests that ICS may be a viable method to coordinate the actions of CSIRTs and first responders. Contemporary research on ICS, as well as government reports on cyber incident management, underscores that new understandings of how ICS may be used in response to SCADA incidents are needed.

## CONTEMPORARY SCHOLARSHIP ON THE INCIDENT COMMAND SYSTEM

Research on ICS tends to emphasize one of three primary themes. First, ICS must be adapted to the unique local circumstances in which it is being used, taking into consideration factors such as the scope of the emergency and the jurisdictions involved in the response. Second, despite the strengths of ICS, the system also suffers from a number of serious deficiencies that may limit its effectiveness under certain conditions. And third, analyses of ICS’s organizational structure show that the system combines elements of vertical organizational hierarchies and horizontal organizational networks, which may prove especially advantageous in responding to SCADA incidents.

Many authors address the customization of ICS to the needs of specific government agencies (Lam et al., 2010; Bauer, 2009; Esposito, 2011; Yates 1999; Ullman, 1998). Other scholars, however, critique ICS for its lack of customizability. For example, at least one author notes that ICS may be unsuitable for response to cyber incidents (Coleman, 2010). Still others take issue with ICS’ inability to address

FIGURE 1: PROTOTYPICAL INCIDENT COMMAND SYSTEM (ICS) STRUCTURE



higher-level command structures beyond that of the incident itself; the very notion that an incident can be controlled within any type of framework; the natural limits of ICS to adapt quickly to especially demanding incidents, such as nuclear, chemical, or biological attacks; ICS' inability to absorb volunteers; its utility being applicable only to para-military types of organizations; and the need for extensive organizational training in order to realize its benefits (e.g. Lutz & Lindell, 2008; Cole, 2000; Favero 1999; Yates, 1999).

A recent notable disaster—the 2010 Deepwater Horizon oil rig explosion and spill—highlights the complex forces influencing field use of ICS and underlines the salience of these observations (Givens, 2011; Baron, 2010). Descriptions of how ICS blends both elements of hierarchies and networks are useful, too, because they can enhance understandings of how ICS can be leveraged for SCADA incident responses (Moynihan, 2007, 2008, 2009, 2009b).

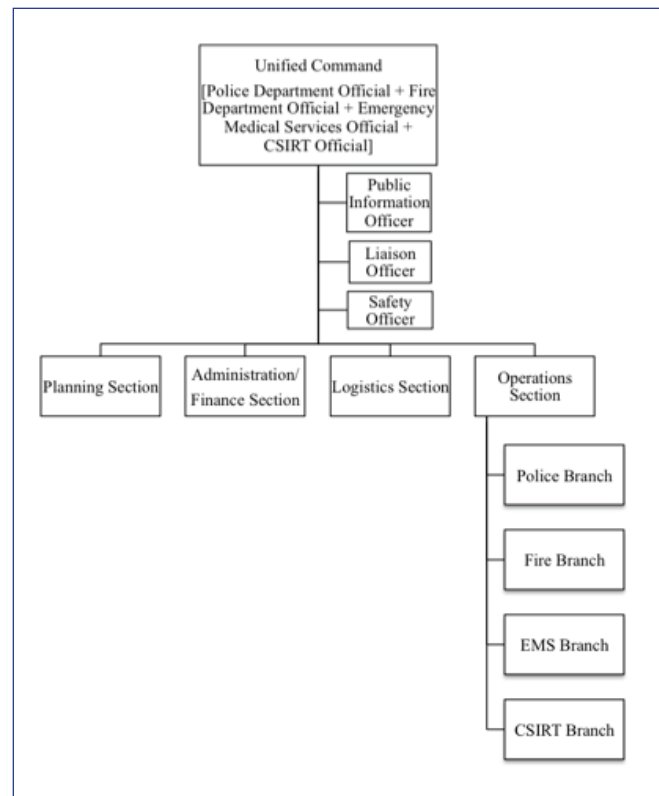
Government reports on recent exercises to evaluate cyber incident responses say nothing about ICS's suitability for emergencies concurrently affecting SCADA systems and the physical world. Indeed, three full-scale exercise reports from DHS spanning 2006–2011 do not specifically mention ICS at all (DHS, 2011; DHS, 2009; DHS, 2006). These documents do, however, underscore the continuing need for improved communication, coordination, and information sharing in response to incidents affecting critical infrastructure in the physical world and cyberspace. In particular, they highlight the unique challenge of maintaining a baseline of situational awareness across all response entities during a large-scale emergency (DHS, 2011; DHS, 2009; DHS, 2006). While greater knowledge of ICS's field-based utility and adaptability is helpful, existing literature fails to explain how CSIRTs and first responders might effectively integrate their actions within an ICS structure during a SCADA incident.

Unfortunately, there do not appear to be any published case studies of how ICS has been used to integrate the actions of one or more CSIRTs and traditional first responders managing a SCADA incident. This is understandable, however, because the idea of CSIRTs and traditional first responders coordinating a shared response to a SCADA incident is still relatively new. But to illustrate how this coordination between a CSIRT and first responders could work, let us next consider a hypothetical example.

## INTEGRATING CSIRTS AND FIRST RESPONDERS USING THE INCIDENT COMMAND SYSTEM

ICS can be modified easily to integrate CSIRTs and first responders into a unified command structure. Figure 2 adjusts the prototypical ICS structure and shows how this integration occurs. For example, let us assume that a computer hacker maliciously attacks a SCADA system regulating the flow of water out of a dam. This electronic attack, in turn, causes the dam to release a torrent of water into a downstream community, causing flooding. Under this scenario, a linkage exists between this cyber attack and its physical effects. A CSIRT will need to manage the cyber attack on the SCADA system and traditional first responders will need to address flooding in this downstream community.

FIGURE 2:  
INCIDENT COMMAND SYSTEM (ICS)  
STRUCTURE—INTEGRATING A COMPUTER  
SECURITY INCIDENT RESPONSE TEAM (CSIRT)  
AND TRADITIONAL FIRST RESPONDERS



The CSIRT integrates into the ICS structure as a branch within the Operations section, visible in the bottom right corner of Figure 2. Additionally, a CSIRT member joins other members of the Unified Command, visible in the top center of Figure 2. CSIRT members in the Operations section work on the cyber component of this incident by managing the hacker's attack on the SCADA system. They work to halt the hacker's progress and to restore the flow of water out of the dam to normal, pre-incident levels. Striving to mitigate a future, similar attack, they examine software code in concert with a vendor to ensure security patches are properly installed. After the incident has ended and recovery has begun, they conduct a formal after-action analysis to confirm that network vulnerabilities have been adequately closed.

While the CSIRT members address the cyber component of this incident, first responders contend with the physical effects of the cyber attack. Police officers re-direct traffic. Firefighters assist with swift water rescue of citizens trapped in their homes. Emergency medical personnel attend to the injured. Each of these distinct responses—the actions taken by the CSIRT, and the actions taken by first responders—forms part of a larger, integrated ICS structure.

ICS is useful for this kind of incident because of its scalability. Responses to SCADA system attacks incidents can involve fuzzy lines of jurisdiction and control, complicating response efforts (DHS, 2011, pp. 17–19; DHS, 2009, pp. 11–12; DHS, 2006, pp. 6–7). Thus a computer server owned by Firm A, manufactured by Firm B, cooled by equipment from Firm C, connected to a computer network via hardware from Firm D, and serviced by contractors from Firms E and F, can control a dam under the jurisdiction of Town G, which is located upstream from Villages H, I, and J. When this server's failure triggers effects in the physical world, it is challenging to organize and coordinate response agencies and organizations. Yet when necessary, ICS rapidly scales geographically, and it can efficiently incorporate these different actors into a unified response effort.

ICS is also helpful in this hypothetical incident because it can successfully integrate the actions of teams performing very different functions. CSIRT

team members and traditional first responders like police officers, firefighters, and emergency medical personnel have divergent professional responsibilities. Since ICS can incorporate diverse groups of responders, including CSIRT team members and traditional first responders, it can be used to bring the efforts of these different functional groups together within a focused response coordination structure.

ICS offers a viable way forward for CSIRTs and first responders to synchronize their response efforts during a SCADA system attack. ICS can easily expand to group CSIRTs and first responders into a unified organizational structure. The system is able to accommodate teams of professionals from numerous organizations and jurisdictions, even when they are spread across a wide geographical area. And ICS permits professionals performing radically different jobs to work together toward common objectives. On its face, ICS appears to offer an effective method for CSIRTs and first responders to collaborate during SCADA system incidents.

Having made the case that ICS offers a potential solution for CSIRTs and first responders to integrate better their responses to SCADA system incidents, the next section argues that ICS training should be an essential component of professional education for cybersecurity professionals.

## BRIDGING THE GAP: INCORPORATING ICS TRAINING INTO CYBERSECURITY CURRICULA

While numerous cybersecurity professional certifications exist, none appear to offer training in ICS. This is puzzling, since DHS has signaled clearly that ICS is the preferred response method for cyber incidents of any size or scope. Moreover, even certifications for those personnel specifically handling cyber incident responses do not appear to include ICS as part of their curricula. Table 1 lists four of the most popular IT security certifications and shows that these certifications do not include training in ICS.

TABLE 1:  
IT SECURITY PROFESSIONAL CERTIFICATIONS AND REQUIREMENTS

CERTIFYING BODY	CERTIFICATION	RELEVANT BASIC TRAINING REQUIREMENTS	EVIDENCE OF ICS TRAINING? (YES/NO)	INFORMATION SOURCE(S)
SANS Institute	GIAC Certified Incident Handler	Incident Handling Overview, Identification, and Containment	No	SANS Institute, 2014
ISC	Certified Information Systems Security Professional (CISSP)	Domain experience in 2 of 10 functional areas, including business continuity/ disaster recovery	No	ISC <sup>2</sup> , 2014; ISC <sup>2</sup> , 2014b
CompTIA	Security +	Access control, identity management, cryptography, mitigation/deterrent techniques	No	CompTIA, 2014
EC-Council	Certified Incident Handler	Incident Response, Incident Handling, Incident Categories	No	EC-Council, ND

The GIAC Certified Incident Handler credential is prestigious, in that it comes from the SANS Institute, one of the most widely recognized and peer-respected cybersecurity organizations (Symantec, 2012). The qualifications for this certification require cybersecurity professionals to show knowledge and proficiency in multiple functional areas, including the “steps of the incident handling process” and “common attack techniques that compromise hosts” (SANS Institute, 2014). These types of functional knowledge are to be expected, since they are indispensable for successful cyber incident management. However, the SANS Institute website detailing the requirements for this credential do not identify knowledge of ICS as a key requirement for the certification.

The CISSP is arguably the most recognizable credential among cybersecurity professionals (Nemeth et al., 2010, p. 945). The process to earn the CISSP is long and rigorous. In addition to passing an exam, prospective CISSP candidates must obtain at least five years of direct, full-time work experience in 2 of 10 knowledge domains (ISC<sup>2</sup>, 2014b). These knowledge domains are: access control; telecommunications and network security; information security governance and risk management; software development security; cryptography; security architecture and design; operations security; business continuity and disaster recovery planning; legal, regulations, investigations,

and compliance; and physical (environmental) security (ISC<sup>2</sup>, 2014b). Of these 10 knowledge domains, the business continuity and disaster recovery domain is most directly applicable to ICS since ICS itself was born out of the need to respond more effectively to traditional disasters, such as fires and earthquakes. Nevertheless, the ISC<sup>2</sup> website does not mention training in ICS at all.

CompTIA’s Security + credential is not viewed universally to be among the strongest security credentials for IT professionals (Anderson, 2010). The credential is still popular, however, due in part to its reasonable cost (Anderson, 2010). The Security + certification covers several fundamental areas of cybersecurity, including access control, identity management, cryptography, incident mitigation, and deterrent techniques (CompTIA, 2014). However, there is no indication on the CompTIA website that ICS training is part of the Security + curriculum. CompTIA also does not appear to offer other certifications that would be more relevant or useful for cyber incident management purposes.

EC-Council’s Certified Incident Handler credential uses a classroom and lab-based learning model over a two-day period (EC-Council, 2014). The organization’s website includes a detailed agenda for the two day training period, and this agenda lists a significant



amount of instruction about how to form CSIRTs, incident response methods, and how to identify and categorize incidents that occur (EC-Council, n.d., pp. 3–6). But nowhere in this detailed training agenda does EC-Council mention ICS, its applicability to cyber incidents, or the ways in which ICS can integrate the efforts of CSIRTs and traditional first responders.

Four of the top cybersecurity professional certifications do not appear to identify or address explicitly the need for cybersecurity professionals to be proficient in ICS. One might expect colleges and universities, which recently have seen a great surge in growth of cybersecurity degree programs, to fill this gap in knowledge by including ICS instruction in their undergraduate and graduate-level curricula. It appears, however, that at least among the top five cybersecurity degree programs in the country, none have incorporated ICS training into their course syllabi.

A 2014 study by the Ponemon Institute, an independent Michigan-based research center focusing on IT security issues, ranked the top collegiate cybersecurity programs in the nation (Ponemon Institute, 2014). The data to construct the rankings came from a survey of IT security practitioners (Ponemon Institute, 2014, pp. 1–2). The top five schools in the rankings, in descending order, were: the University of Texas at San Antonio, Norwich University, Mississippi State University, Syracuse University, and Carnegie Mellon University (Ponemon Institute, 2014, p. 1). A web-based survey of these institutions’ cybersecurity curricula suggests that ICS training is not being included in higher education curricula for cybersecurity. Table 2 lists the top five schools in the Ponemon Institute rankings, identifies classes within their curricula that relate to incident responses, and identifies those institutions that explicitly include ICS as part of their coursework.

TABLE 2:  
TOP 5 ACADEMIC CYBERSECURITY PROGRAMS AND ICS TRAINING \*

INSTITUTION	RELEVANT DEGREE PROGRAM(S) OFFERED	COURSE(S) RELATED TO CYBER INCIDENT MANAGEMENT	EVIDENCE OF ICS TRAINING BEING OFFERED? (YES/NO)	SOURCE(S)
UNIVERSITY OF TEXAS AT SAN ANTONIO	BBA Cybersecurity, MS Information Assurance, BS and MS in Computer Science with security concentration	Principles of Computer Information Security, Introduction to Digital Forensics, Intrusion Detection and Incident Response	No	UTSA, n.d.; UTSA, n.d.-b; UTSA, n.d.-c; UTSA, n.d.-d; UTSA, n.d.-e
NORWICH UNIVERSITY	Computer Security and Information Assurance undergraduate major and minor	Information Assurance I and II	No	Norwich University 2014; Norwich University 2014b
MISSISSIPPI STATE UNIVERSITY	BS Computer Science, BS Software Engineering, MS Computer Science	Business Information Systems Security Management	No	MSU, 2014; MSU, 2014b; MSU, 2013
SYRACUSE UNIVERSITY	MS Cybersecurity, Certificate of Advanced Study in Information Security Management	Computer Security, Internet Security	No	SU, 2015; SU, 2015b
CARNEGIE MELLON UNIVERSITY	MS Information Security	Network Forensics, Cyber Forensics and Incident Response Capstone	No	CMU, 2014; CMU, 2014b

\* AS CALCULATED IN PONEMON, 2014.

The University of Texas at San Antonio houses the top-ranked cybersecurity degree programs in the United States (Ponemon Institute, 2014, p.1). These programs include a Bachelor of Business Administration degree in Cybersecurity, as well as a Master of Science degree in Information Assurance (UTSA, n.d.-b; UTSA, n.d.-c). UT San Antonio features several courses that pertain to cyber incident management, as well. These courses include Introduction to Digital Forensics, which teaches students how to analyze systematically the aftermath of a cyber incident, as well as Intrusion Detection and Incident Response, which deals precisely with the topic of responding to cyber incidents (UTSA, n.d.-e). Among the descriptions of these degree programs and courses, however, there is no mention of ICS. Norwich University, Mississippi State University, Syracuse University, and Carnegie Mellon University round out the top five cybersecurity academic programs in the United States. None of these institutions appears to offer any instruction in ICS for cybersecurity students, either.

There are several possible explanations for the absence of ICS instruction in these top cybersecurity degree programs. The simplest and most plausible explanation is that these institutions *do* train students in ICS within their courses, but they do not make that fact publically known on their websites. It is also possible that universities are reacting to changing marketplace demands in cybersecurity, and this reacting creates a lag effect between the emergence of a market-driven need for training in ICS and universities ultimately incorporating ICS training into their curricula. This explanation seems less probable, though. The NCIRP, which specifically identified ICS as the response method of choice, was published in 2010—four years before this writing, and a reasonable amount of time for universities to adopt and incorporate ICS training into their courses. A third possible explanation is that training in ICS is seen as too “practitioner-driven” for a university setting and somehow lacking in academic rigor or legitimacy. Yet this explanation rings hollow, as Norwich University and Syracuse University are known for being “military-friendly” institutions with many students that come from practitioner-oriented backgrounds in the U.S. armed services (Jevis, 2014; Norwich, 2014).

It is clear that the top cybersecurity professional certifications and cybersecurity academic programs in the United States either do not include ICS training as part of their course curricula; or, at a minimum, these certifications and degree programs do not place great emphasis on the fact that this ICS training is included in their courses. Given the need for CSIRTs and first responders to synchronize their responses to SCADA incidents, this gap in ICS training should be corrected by the certifying bodies and universities themselves. To support these certifying bodies and universities in their efforts, however, DHS and the Department of Defense (DOD) can offer three forms of low- or no-cost assistance.

DHS and DOD can help to push knowledge of ICS to cybersecurity certification groups and universities through incentives, web-based resources, and hands-on training. If it costs certification organizations money to make changes to their curricula, then they must have a compelling reason to make these modifications. DHS and DOD can offer one-time cash awards, in the form of grants or prizes, to groups like ISC<sup>2</sup> and institutions of higher education to make these changes quickly. This “free money” would go a long way toward overcoming organizational inertia to making curricular modifications, and would not act as a long-term financial burden on the federal government, because the awards themselves would be one-time-only cash allocations. DHS and DOD can also make available web-based resources for ICS training. DHS already makes available online ICS resources for first responders and others in the emergency management community (DHS, ND). Tailoring this information slightly to a cybersecurity-oriented audience could be helpful in encouraging CSIRTs to adopt ICS. Lastly, DHS and DOD could offer occasional hands-on training in ICS for CSIRTs. To encourage attendance, these agencies would have to offer the training so that it is convenient for CSIRTs to attend, and at little or no cost. DHS already conducts these hands-on ICS trainings, often through state-level emergency management agencies, for first responders and emergency managers (VDEM, 2012). Adapting the existing hands-on ICS training for CSIRTs could also go a significant way toward encouraging CSIRTs to adopt ICS.

## CONCLUSIONS

This article argued that CSIRTs should use ICS during SCADA incidents, because doing so makes it easier to integrate CSIRT actions with those of traditional first responders. Although this arrangement may present select communication and coordination challenges for CSIRTs and first responders, on balance ICS will help CSIRTs and first responders to manage SCADA incidents more effectively. To facilitate the use of ICS by CSIRTs, the nation's top professional cybersecurity certification groups and universities offering cybersecurity degrees should make ICS an explicit part of their curricula.

There is a compelling need for additional research in this area, because little is known about the process by which the field-based findings of homeland security and cybersecurity practitioners eventually integrate into educational and training programs. In particular, the absence of case studies about how lessons learned from specific incident responses feed into educational programs in homeland security and cybersecurity is problematic. Scholars and practitioners can benefit from deeper investigations of how these lessons learned in real world incidents can be integrated better into formal educational settings.

The cybersecurity and emergency management communities can also benefit from greater knowledge exchange. It has been said that ICS can be a way of thinking about incident management, as well as a way of coordinating response to an incident. In other words, ICS is not merely a management tool for dealing with an incident; ICS also conveys a cultural approach to incident management that emphasizes principles like flexibility, adaptability, and creativity. How can CSIRTs learn to “do” ICS, and also embrace these principles in their own cultural approach to incident management?

One possible first step is for CSIRT members in government agencies and the private sector to take independent study courses online through the Federal Emergency Management Agency's (FEMA) Emergency Management Institute as part of their normal training activities. These emergency management courses, which are available for free, can provide CSIRT members with introductory knowledge of the principles found in NIMS, the NRF, and ICS (FEMA, 2012). In completing these courses, CSIRT

members can develop more sophisticated and nuanced understandings of how ICS can be beneficial for them. CSIRT members can also gain helpful insights into how first responders use ICS during incidents. Important principles of emergency management like flexibility and resiliency can become more inculcated in a CSIRT's culture as a result of this training. And this training, in turn, can help CSIRTs to better integrate their operations with traditional first responders, and to achieve better results in managing incidents.

As SCADA incidents become increasingly common, there will be a pressing need for CSIRTs and traditional first responders to coordinate their response actions. ICS, a proven method for managing incidents of any size, scope, or cause, can help CSIRTs and first responders to better integrate their efforts and strengthen homeland security as a result. It is now essential that cybersecurity training and education programs embrace ICS to prepare their students for joint responses with homeland security practitioners.

## REFERENCES CITED

- Anderson, N. (2010, January 26). Thought that A+ cert was good for life? Think again. *Ars Technica*. Retrieved from <http://arstechnica.com/tech-policy/2010/01/thought-that-a-cert-was-good-for-life-think-again/>
- Bauer, T.P. (2009). *Is NIMS going to get us where we need to be?: A law enforcement perspective* (master's thesis). Naval Postgraduate School, retrieved from the Homeland Security Digital Library.
- Baron, G. 2010. (2010, May 14). Deepwater and the future of NIMS. *Emergency Management*. Retrieved from <http://www.emergencymgmt.com/emergency-blogs/crisis-comm/Deepwater-and-the-Future.html>
- Barzashka, I. (2013). Are cyber weapons effective? Assessing Stuxnet's impact on the Iranian enrichment program. *The RUSI Journal*, 158, 48–56.
- Carnegie Mellon University. (2014). CyLab. Retrieved from <https://www.cylab.cmu.edu/education/index.html>
- Carnegie Mellon University. (2014b). MSIS Core Course Descriptions. Retrieved from <http://www.ini.cmu.edu/degrees/msis/courses.html#forensics>
- Cole, D. (2000). *The Incident command system: A 25 year evaluation by California practitioners*. Retrieved from <http://www.usfa.fema.gov/pdf/efop/efo31023.pdf>
- Coleman, K. (2010, October 18). Cyber incident responders lack a shared playbook. *DefenseSystems*. [Commentary]. Retrieved from <http://defensesystems.com/articles/2010/10/15/digital-conflict-cyber-incident-response.aspx>
- CompTIA. (2014). CompTIA Security +. Retrieved from <http://certification.comptia.org/getCertified/certifications/security.aspx>

- C-SPAN. (2011, March 16). Louisiana Incident Command Post. Retrieved from [http://youtu.be/\\_ctvFT\\_Sq7w](http://youtu.be/_ctvFT_Sq7w)
- DeAtley, C. (2011). 45 seconds of danger, a lifetime of lessons. *DomPrep Journal*, 7, 12–13.
- Department of Homeland Security. (2014). *Cyber storm: Securing cyber space*. Retrieved from <http://www.dhs.gov/cyber-storm-securing-cyber-space>
- Department of Homeland Security. (2011). *Cyber storm III: Final report*. Retrieved from <http://www.dhs.gov/sites/default/files/publications/CyberStorm%20III%20FINAL%20Report.pdf>
- Department of Homeland Security. (2010). *National cyber incident response plan [Interim Version]*. Retrieved from [http://www.federalnewsradio.com/pdfs/NCIRP\\_Interim\\_Version\\_September\\_2010.pdf](http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf)
- Department of Homeland Security. (2009). *Cyber storm II: Final report*. Retrieved from <http://www.dhs.gov/sites/default/files/publications/Cyber%20Storm%20II%20Final%20Report.pdf>
- Department of Homeland Security. (2008). *National incident management system* [Brochure]. Retrieved from [http://www.fema.gov/pdf/emergency/nims/NIMS\\_brochure.pdf](http://www.fema.gov/pdf/emergency/nims/NIMS_brochure.pdf)
- Department of Homeland Security. (2008b). *National incident management system*. Retrieved from [https://www.fema.gov/pdf/emergency/nims/NIMS\\_core.pdf](https://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf)
- Department of Homeland Security. (2006). *Cyber storm exercise report*. Retrieved from <http://www.dhs.gov/sites/default/files/publications/Cyber%20Storm%20I%20After%20Action%20Final%20Report.pdf>
- Department of Homeland Security. (2003, February 28). *Homeland Security Presidential Directive 5: Management of Domestic Incidents*. Retrieved from <http://www.dhs.gov/sites/default/files/publications/Homeland%20Security%20Presidential%20Directive%205.pdf>
- Department of Homeland Security. (n.d.). *ICS resource center*. Retrieved from <http://training.fema.gov/EMIWeb/is/ICSResource/>
- EC-Council. (2014). *EC-Council certified incident handler*. Retrieved from <http://www.eccouncil.org/Certification/ec-council-certified-incident-handler>
- EC-Council. (n.d.). *EC-Council certified incident handler course outline, Version 1*. Retrieved from <http://www.eccouncil.org/portals/0/Images/img/icons/ECH-v1-Course-Outline.pdf>
- Esposito, J.M. (2011). *New York City chief fire officer's evaluation of the citywide incident management system as it pertains to interagency emergency response* (master's thesis). Retrieved from the Homeland Security Digital Library.
- Favero, G.T. (1999). *Flexibility of the incident command system to respond to domestic terrorism* (master's thesis). Retrieved from the Homeland Security Digital Library.
- Federal Emergency Management Agency. (2012). *Emergency management institute: Independent study program*. Retrieved from <http://training.fema.gov/is/>
- Ferran, L. & Radia, K. (2013, July 9). *Edward Snowden: U.S., Israel 'co-wrote' cyber super weapons Stuxnet*. ABC News. Retrieved from <http://abcnews.go.com/blogs/headlines/2013/07/edward-snowden-u-s-israel-co-wrote-cyber-super-weapon-stuxnet/>
- Fildes, J. (2010, September 23). *Stuxnet worm 'targeted high-value Iranian assets'*. BBC. Retrieved from <http://www.bbc.com/news/technology-11388018>
- Givens, A. (2011, May 27). Deepwater Horizon oil spill is an ominous sign for critical infrastructure's future. *Emergency Management*. Retrieved from <http://www.emergencymgmt.com/disaster/Deepwater-Horizon-Oil-Spill-Critical-Infrastructure-052711.html?page=1&>
- ISC<sup>2</sup>. (2014). *How to get your CISSP certification*. Retrieved from <https://www.isc2.org/cissp-how-to-certify.aspx>
- ISC<sup>2</sup>. (2014b). *CISSP-professional experience requirement*. Retrieved from <https://www.isc2.org/cissp-professional-experience.aspx>
- Jevis, E. (2014, January 13). *SU selected as a top military-friendly school*. Retrieved from <http://news.syr.edu/su-selected-as-a-top-military-friendly-school-61362/>
- Katz, Y. (2010, December 15). Stuxnet virus vet back Iran's nuclear program by 2 years. *The Jerusalem Post*. Retrieved from <http://www.jpost.com/Iranian-Threat/News/Stuxnet-virus-set-back-Irans-nuclear-program-by-2-years>
- Lam, C., Lin, M., Tsai, S., & Ta-Chiu, W. (2010). A pilot study of citizens' opinions on the incident command system in Taiwan. *Disasters*, 34, 447–469.
- Lutz, L.D. & Lindell, M.K. (2008). Incident Command System as a Response Model Within Emergency Operations Centers during Hurricane Rita. *Journal of Contingencies and Crisis Management*, 16, 122–134.
- Mississippi State University. (2014). Department of Computer Science and Engineering: Academics [Course listing]. Retrieved from <http://www.cse.msstate.edu/academics/understud/>
- Mississippi State University. (2014b). Center for Computer Security Research [Course listing]. Retrieved from <http://www.security.cse.msstate.edu/academics.php>
- Mississippi State University. (2013). Department of Computer Science and Engineering: Prospective Students. Retrieved from <http://web.cse.msstate.edu/prospective/grad/msguidelines.php>
- Moynihan, D. P. (2009). The network governance of crisis response: Case studies of incident command systems. *Journal of Public Administration Research and Theory*, 19, 895–915.
- Moynihan, D. P. (2009b). From intercrisis to intracrisis learning. *Journal of Contingencies and Crisis Management*, 17, 189–198.
- Moynihan, D. P. (2008). Combining structural forms in the search for policy tools: Incident command systems in U.S. crisis management. *Governance: An International Journal of Policy, Administration, and Institutions*, 21, 205–229.
- Moynihan, D. P. (2007). *From forest fires to Hurricane Katrina: Case studies of incident command systems*. IBM Center for the Business of Government. Retrieved from the Homeland Security Digital Library.

National Security Archive. (2013, April 26). *Update: Agent Farewell and the Siberian pipeline explosion*. Retrieved from <https://owl.english.purdue.edu/owl/resource/560/10/>

Nemeth, E., Snyder, G., & Hein, T.R. (2010). *Unix and Linux system administration: 4th edition*. Upper Saddle River, NJ: Prentice Hall.

The 9/11 Commission. (2004). *The 9/11 Commission Report*. Retrieved from <http://www.9-11commission.gov/report/911Report.pdf>

Norwich University. (2014). BS in Computer Security and Information Assurance [Course listing]. Retrieved from <http://profschools.norwich.edu/business/csia/curriculum/>

Norwich University. (2014b). Information Assurance Minor [Course listing]. Retrieved from <http://profschools.norwich.edu/business/csia/information-assurance-minor/>

Ponemon Institute. (2014). *2014 best schools for cybersecurity*. Retrieved from [http://www.hp.com/hpinfo/newsroom/press\\_kits/2014/RSAConference2014/Ponemon\\_2014\\_Best\\_Schools\\_Report.pdf](http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_2014_Best_Schools_Report.pdf)

SANS Institute. (2014). GIAC Certified Incident Handler (CIH). Retrieved from <http://www.giac.org/certification/certified-incident-handler-gcih>

Symantec. (2012, December 18). *Security bulletin from SANS Institute*. Retrieved from <http://www.symantec.com/connect/blogs/security-bulletin-sans-institute>

Syracuse University. (2015). Academic Programs: Cybersecurity. Retrieved from <http://eng-cs.syr.edu/prospective-students/academic-programs/masters/detail/cybersecurity>

Syracuse University. (2015b). 2015–2016 Graduate Course Catalog: Certificate of Advanced Study in Information Security Management [Course listing]. Retrieved from [http://coursecatalog.syr.edu/preview\\_program.php?catoid=4&pooid=1521](http://coursecatalog.syr.edu/preview_program.php?catoid=4&pooid=1521)

Ullman, M. (1998). *Integration of the incident management system between the police and fire departments of the city of Goodyear, Arizona*. Retrieved from the Homeland Security Digital Library.

University of Texas at San Antonio. (n.d.). *UTSA Cyber Security*. Retrieved from <http://utsa.edu/cybersecurity/>

University of Texas at San Antonio. (n.d.-b). Bachelor of Business Administration Degree in Cyber Security [Course listing]. Retrieved from <http://www.utsa.edu/ucat/cob/bbaia.html>

University of Texas at San Antonio. (n.d.-c). Master of Science Degree in Information Technology–Information Assurance Concentration [Course listing]. Retrieved from <http://www.utsa.edu/gcat/chapter6/COB/istmdept.html#msitiac>

University of Texas at San Antonio. (n.d.-d). Dependency graph of required CS courses and concentrations: 2014–2016 catalog. Retrieved from [http://www.cs.utsa.edu/uploads/docs/CSCoursesForMajorsConcentrations\\_2014.pdf](http://www.cs.utsa.edu/uploads/docs/CSCoursesForMajorsConcentrations_2014.pdf)

University of Texas at San Antonio. (n.d.-e). Information Systems (IS) Course Descriptions. Retrieved from <http://www.utsa.edu/ucat/cob/is.html#is3523>

VDEM. (2012). *ICS-400: Advanced Incident Command System*. Retrieved from <http://www.vaemergency.gov/em-community/training/ics-400-advanced-ics-400>

Warrick, J. (2011, February 16). Iran's Natanz nuclear facility recovered quickly from Stuxnet cyber attack. *The Washington Post*. Retrieved from <http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html>

Yates, J. (1999). Improving the management of emergencies: enhancing the ICS. *Australian Journal of Emergency Management*, Winter, 22–28.

---

## AUTHOR

---

**Austen D. Givens** ([adgivens@utica.edu](mailto:adgivens@utica.edu)) is an assistant professor of cybersecurity at Utica College and a doctoral candidate at King's College London. With Nathan E. Busch, he is the author of *The Business of Counterterrorism: Public-Private Partnerships in Homeland Security* (2014). Follow him on Twitter @GivensAD.





