Job Training in Cybersecurity by Dartmouth and River Valley Community College

Electronic health records (EHRs) promise quality and continuity of medical treatment as a patient moves from one provider setting to another, streamlined record keeping, and overall health care cost containment. But public concerns over privacy and security are creating the need for new technicians with specialized expertise in order to deal with these issues.

Dartmouth and River Valley Community College will work together to help provide the advanced training needed to produce a local workforce with the skills and knowledge to install, operate, secure, and maintain systems in support of EHR implementation.

Testing Assumptions About Security Awareness

When 10,000 New York state employees were sent a phishing email, three-quarters of them opened it, and 17 percent clicked on the embedded link. Fifteen percent even supplied requested passwords and confidential data! Stories like this suggest that once-a-year, slide-set-based computer security training doesn't work: people still write down passwords, click on links in emails from untrusted sources, and download software with unknown provenance.

To address this problem, an I3P team from MITRE and Dartmouth College implemented immediate training and examined its effects. In a series of studies, the team sent spear phishing emails to several thousand recipients participating at companies and universities. A recipient in the control group clicking on the embedded link was told that she had just been spear phished. In the treatment groups, the clicking recipient was also presented with a training page describing what spear phishing is, how to recognize possible phishing emails and misleading links, and how to report suspicions to the help desk.
Dartmouth Partners
...continued from page 1

Dartmouth and River Valley Community College (RVCC) in Claremont, N.H., will work together to help provide the advanced training needed to produce a local workforce with the skills and knowledge to install, operate, secure, and maintain systems in support of EHR implementation. Dartmouth’s part in this joint effort will be led by the I3P.

The collaborative educational project, “Program Development in Cybersecurity with Focus on Business and Healthcare Concepts,” is being funded with $400,000 from the National Science Foundation’s Advanced Technological Education (ATE) program. The project’s goal is to produce well-qualified science and engineering technicians for advanced technological fields, as well as to train effective teachers for these subjects at the undergraduate level.

“Dartmouth has a history of interest and innovation in information technology,” says Dartmouth Vice Provost Martin Wybourne. “We are pleased with the opportunity to share our knowledge and contribute to training the next generation of technical experts in our rural northern New England community.”

River Valley Community College, the lead institution on the project, will use the grant to develop an Information Assurance Certificate and an Information Assurance Associate of Science degree with a specialized focus on the needs of the health care industry. The curriculum will eventually extend to other campuses in the Community College System of New Hampshire.

Steve Budd, president of RVCC, says “This project represents a model of collaboration where knowledge transfer from major research universities becomes cutting edge curricula for educating technicians and technologists.”

Dartmouth will provide support to the ATE project through the expertise of I3P member institutions by integrating content in information assurance and business skills into RVCC’s technician level training.

“The I3P’s breadth of expertise in information technology will be instrumental in the development of this program,” says I3P Executive Director Martha Austin. “In addition, many of our researchers teach at the undergraduate level and can contribute their experience to create an effective program.”

-Article by Joseph E. Blumberg, Dartmouth Now

Testing Assumptions
...continued from page 1

The study aimed to reveal when training is most effective. Effectiveness was measured in several ways, including clicking links and reporting problems to the help desk. The treatments varied in framing the training page’s information: as an individual vs. community benefit, and as a gain vs. a loss. These treatment types are based on a well-respected body of behavioral science literature documenting significant differences in reaction to framing; the problem and choices are presented identically except for the framing, so that testing can reveal choices that react only to the framing.

The result? The training pages did not change the clicking and reporting rates in any statistically significant way. The I3P hopes to explore the reasons for this surprising result. Perhaps today’s IT workers are too busy to read the training page; the next study will measure whether it is open long enough for someone to read it. Perhaps workers think it is

“I3P Researchers in the News

Bruce Balds of the MITRE Corporation is mentioned in an article on privacy audits.
-Forbes

Idaho National Laboratory is featured in an NPR story on Stuxnet and cyberwar.
-NPR

Georgia Tech’s Steve Lukasik has recently written cover stories for both IEEE and Communications of the ACM.
-IEEE and Communications of the ACM”
Sujeet Shenoi of Tulsa University and National Security Agency's Dickie George are cited in an article on security for the U.S. power grid. -IT Business Edge

Purdue University's Marc Rogers is interviewed in a New Scientist article on Internet hacker groups. -New Scientist

Cyber Security CPR Workshop and Webinar Address Tough Problems in Private/Public Relationships

What happens when a cyber incident brings down something essential to public welfare? Since much of the US's critical infrastructure is privately-owned, who is responsible for planning a response to a cyber attack? In what situations can government direct private enterprise to take action? These are just three of the many questions facing public and private sector practitioners, policy-makers, and researchers. Over the last two decades, these communities have combined expertise in IT and risk management to meet these challenges in incident response.

Last Fall, to explore appropriate incident response, the I3P and the CERT® Program at Carnegie Mellon University's Software Engineering Institute organized a workshop on Cyber Security CPR: Coordinated Private Sector Responses to Cyber Security Incidents. The workshop was preceded by an online webinar. A first for the I3P, the webinar allowed participants to attend an informative presentation without ever having to leave their desks. Participants watched as experts explained major cyber events, including the Morris Worm, Conficker, and Stuxnet. Participants then engaged the presenters and asked questions in real-time in the virtual environment. The session was recorded and is available to view on the I3P website at: http://www.thei3p.org/events/cybercprwebinar.html.

The online webinar was a success in adding historical context for the main workshop, held on October 12th and 13th in Arlington, VA. The Cyber Security CPR workshop brought experts from private, public and academic sectors to discuss how best to handle cyber events that occur on private networks but have an effect on public welfare. Participants engaged in brainstorming sessions and listened as presenters from both public and private sectors framed the problem. Issues tackled during the workshop included determining if and when the public sector should get involved with cyber response, how to facilitate information sharing without compromising sensitive data, identifying critical research areas to enhance cyber response, and recommending potential issues to be addressed in legislation.


Upcoming Events

March 19-21, 2012
Sixth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection
Washington, D.C.

June 6, 2012
Privacy Workshop: Perceptions, Policies and Trade-offs
Washington, D.C.

For more information on these and other events, visit http://www.thei3p.org/events/

I3P Researchers in the News

Purdue University's Marc Rogers is interviewed in a New Scientist article on Internet hacker groups. -New Scientist


Sujeet Shenoi of Tulsa University and National Security Agency's Dickie George are cited in an article on security for the U.S. power grid. -IT Business Edge

To view these news articles and more, please visit: http://www.thei3p.org/news/researchersinthenews.html
Upcoming Events

March 19–21, 2012
Sixth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection
Washington, D.C.

June 6, 2012
Privacy Workshop: Perceptions, Policies and Trade-offs
Washington, D.C.

For more information on these and other events, visit http://www.thei3p.org/events/

For more information, contact kiel.h.alarcon@dartmouth.edu
To subscribe or unsubscribe send an email to kiel.h.alarcon@dartmouth.edu with the subject line “Add/Remove I3P Newsletter Subscription”