Sautter Award Application - 2018

Project title: Cyber Strong UC: Year-Round Information Security Awareness Campaigns

Project timeframe:

- Initial timeframe: September 2017-September 2018
- Ongoing: Annual review and update of materials

Submitter: Julie Goldstein, IT Security Analyst, UC Cyber-Risk Coordination Center, julie.goldstein@ucop.edu, 510-287-3317

Project team members:

Maurice Anderson, UCD Health	Kamika Hughes, UCOP (backup for project leader)
Kip Bates, UCSB	Dewight Kramer, UCD
Petr Brym, UCD	Alexa Rivetti, UCOP
Cecelia Finney, UCLA	Tamara Santos, UCSC
Julie Goldstein, UCOP – project leader	Esther Silver, UCSF
Bill Green, UCR	Marissa Ventura, UCSD Health
David Hatter, UC ANR	Ronise Zenon, UCSD

Summary: Despite efforts to protect electronic information and systems through technology and education, UC locations continue to see information compromises and breaches. Annual training is not sufficient to change people's behaviors, and each UC location is working with limited resources to develop and run their own information security awareness (ISA) program.

The Systemwide Information Security Awareness Workgroup, which includes representatives from 12 UC locations, experienced extraordinary success working together to create systemwide campaigns for National Cyber Security Awareness Month (NCSAM) in October 2016 and 2017. We were able to develop and provide resources and materials that far exceeded what the individual locations would have been able to do on their own. For the "Cyber Strong UC" project, we decided to extend the NCSAM model and collaboratively develop a series of themed ISA campaigns available to all UC locations, facilitating a year-round, systemwide approach to ISA.

The project has been running for almost a year, producing 6 themed ISA campaigns. Testimonials from individuals responsible for ISA at their locations have been extremely positive (see "Measures of effectiveness" below), as has other direct and indirect feedback. Once again, we have found that by working together, we can all do our jobs better and better support the UC community.

PROJECT DESCRIPTION:

Overview:

The focus of the "Cyber Strong UC" project is to collaboratively develop and share ideas, materials, and other resources for building good cybersecurity habits and promoting information security awareness year-round.

The specific deliverables of this project are a one-year calendar of information security awareness themes, and the development and distribution of ready-to-use and customizable ISA materials and

resources to all UC locations. Materials and resources are compiled into themed "toolkits" for use according to the calendar or as-needed by each location. Locations are free to pick and choose materials from the toolkits and use them as-is or customize them according to their needs.

Problem statement:

This project was prompted by several fundamental problems:

1. UC locations continue to see information compromises and breaches – both actual and near misses – that could be avoided by individuals in the university community consistently following safer practices with respect to electronic information, electronic communications, and online behavior. This is coupled with the trend of attackers increasingly targeting individuals, and the increased sophistication of those attacks. Phishing is one example.
2. The ISA Workgroup believes in the importance of education and awareness to help address the issues in Problem #1 above. In some cases, education and awareness are also required by law or regulation. Once-a-year ISA training is not sufficient to actually raise awareness or change behaviors long-term for most individuals. Several of the ISA Workgroup members and some CISOs were interested in expanding their awareness programs beyond once-a-year efforts (NCSAM and the annual information security awareness training that UC employees are required to complete), but didn't have the resources, bandwidth and/or experience to do so.
3. Every UC location doing its own awareness program from scratch was both resource intensive and missed opportunities to leverage the work and experience of other locations. Sharing was mostly ad-hoc. In most cases, programs also tended to be reactive instead of proactive, largely due to limited resources. Even the few locations with mature year-round awareness programs were on their own to maintain their programs and keep them current.

After making progress on many of its initial goals, the ISA Workgroup decided that in light of the above issues, it made sense to pool our efforts and develop a proactive, year-round information security awareness program that the ISA Workgroup and all other UC locations could leverage. This would allow locations to focus their time and resources on addressing their specific awareness needs (or other needs) instead of on developing basic ISA campaign materials. It would also be a huge help for locations with no real awareness outreach program, or few resources to develop one.

Getting started:

The ISA Workgroup officially launched this project in September 2017 after the 2017 NCSAM toolkit was published. After some brainstorming, we decided to come up with a calendar of ISA themes that would be topical and timely – approximately one theme every two months. Most themes would relate to the time of year, such as holiday online shopping cybersecurity (November/December), W-2 scams (January), and data privacy for Data Privacy Month (February). Other critical themes, such as phishing awareness, would fill gaps in the calendar.

We also decided to follow the model we had developed for NCSAM 2017, though on a smaller scale, and create a series of "toolkits" of ready-to-use and customizable ISA materials and resources. Each toolkit would focus on a single theme, determined by the calendar. Depending on the topic and availability of materials, the toolkits would consist of any or all of the following: articles, posters, videos, social media posts/tweets, webinars and in-person events, informational web pages, tip sheets, and more. Sample screenshots are included at the end of this document.

Our actual process for this project developed through some trial-and-error. We created the calendar of themes in a single brainstorming session, but figuring out how to create the toolkits was a challenge.

Since the whole point was to save locations time and effort, it did not make sense for ISA Workgroup members to spend tons of time on each toolkit. It also didn't make sense for UCOP to develop the materials without workgroup input.

Collaboration is the key – and also the innovation:
In the end, we landed on the following process. It is highly collaborative, and no one individual ends up doing too much:

- The UCOP project leader compiles resources and materials for consideration for each toolkit – typically from around the UC system and partner organizations.
- The ISA Workgroup decides together what we want to use and apportions the content. Members sign up for a section to review, edit, supplement, etc., and make recommendations back to the group.
- We try to strike a balance between external materials, which are often readily available but not necessarily suited to our needs; updating pre-existing materials from the various UCs; and developing new content, which is time-intensive.
- When the ISA Workgroup collectively agrees on the content, the project leader cleans everything up, runs it past the UC Systemwide CISO for final approval, and posts the material on the systemwide ISA website and in the workgroup's UCSF-hosted Box collection for systemwide use.
- Additional sharing includes notifying the UC IT Policy and Security (ITPS) Community of Interest when new awareness campaign materials are available. Some materials are also shared systemwide through UCnet, the UC IT Blog, and the Compliance Alert newsletter produced by Ethics, Compliance and Audit Services (ECAS).

In addition to the cross-campus collaboration of the ISA Workgroup members, this project creates exciting new opportunities for broader collaboration and partnerships. For example:

- In order to develop the Data Privacy campaign, the workgroup consulted and collaborated with the systemwide Privacy Officials, potentially creating a new annual partnership.
- The Digital Spring Cleaning campaign was the impetus for collaboration with UCOP Records Management – both on the article for the toolkit, and bringing information security representation to the Records Management Committee.
- We regularly contribute articles to UCnet, the UC IT Blog, and ECAS' Compliance Alert newsletter (mentioned above).
- We have also had several external requests to use our ISA materials, including from the State of California, the Federal Department of Transportation, and Mount Saint Vincent University in Halifax, Nova Scotia.

This broader collaboration is indicative of the perceived value of the ISA Workgroup's work.

Innovation:
As described above, all project deliverables are developed collectively and are shared among the ISA Workgroup members and all UC locations. In our experience, this is a highly innovative approach at UC. In a very real sense, this collaboration and sharing ***is*** the innovation. ISA campaigns in and of themselves are not new. While the toolkit approach may be somewhat unique, it is the collaborative way the ISA Workgroup is approaching this project – and all of its work – that is creative and innovative. As a group, not only are we able to come up with more ideas and stronger results than we might on our own, our work can benefit the entire UC community and beyond, not just the immediate workgroup.

Deliverables (as-of May 2018):
To-date, we have developed the following ISA materials and toolkits as part of this project:

- Calendar of ISA themes to guide toolkit development and proactive outreach
- Toolkit: Cybersecurity for the Holiday Online Shopping Season (Nov-Dec 2017)
- Article: Protect Yourself from Tax Scams (Jan 2018)
- Toolkit: Data Privacy (Jan-Feb 2018)
- Toolkit: Phishing Awareness (Mar 2018)
- Toolkit: Digital Spring Cleaning (Apr 2018)
- Toolkit: Travel Cybersecurity (May/Jun 2018)
- Scheduled:
    - Toolkit: Beginning-of-the-Year Cybersecurity (mid-Aug 2018)
    - Toolkit: National Cyber Security Awareness Month (Oct 2018) (archive from previous years)

Impact: Our goal, and actual result, is threefold:

1. **Provide themed materials and resources that UC locations can use as-is or with customization to run ISA campaigns year-round according to a pre-established systemwide calendar.** This is especially useful for locations that want to standardize on a systemwide calendar, are just developing their ISA programs, and/or have few resources to devote to an ISA program.
2. **Develop a repository of ISA toolkits that UC locations can use whenever they want or need.** Ultimately, we will have a full year's repository of ISA campaigns that will be updated on an annual basis. This is especially useful for locations that already have an established ISA program. The repository can provide always-available, current, customizable materials so they don't have to develop all of their materials in-house, allowing them to focus their time and resources on addressing their specific awareness needs. The repository is also useful for locations that want to address the systemwide themes on their own schedule.
3. **Save everyone time and resources, and share broadly.** The systemwide ISA Workgroup is pooling our resources to develop this year-round ISA program – doing more than we each could individually with hopefully less effort. And the awareness tools that we are developing are available to the UC community and beyond, not just to ISA Workgroup members.

The overarching impact of this project also extends beyond these immediate results. As part of her strategy for systemwide cyber-related culture change, President Napolitano directed each UC location to appoint a Cyber-Risk Responsible Executive (CRE) responsible for strengthening cybersecurity at their respective locations. This project directly supports the President's strategy and the location CREs by facilitating a year-round, systemwide approach to ISA. UC's employees and students are our first line of cyber defense. Providing year-round education on good cybersecurity practices and current threats will allow the university to be more resilient to the threats we face.

Measures of effectiveness:
Ultimately, the goal of this collaboration, and these toolkits, is to save time and effort by providing a range of resources from which to pick and choose in support of ISA efforts year-round. Examples of effectiveness include:

- UCSB: Testimonial from the UCSB ISA Workgroup representative: "Here at UCSB there has been a 75% time reduction in preparing Cybersecurity Awareness materials and an increase of 500% in Awareness materials being presented at our campus just from participating in this initiative. This has enabled us to extend the depth and breadth of our Awareness program on campus

without increasing local resources. An unexpected outcome from participation in this workgroup is the communication, collaboration and camaraderie of like-minded professionals across the system; this has been priceless."

- UCSF: Approximate quote from the UCSF ISA Workgroup representative regarding the time-saving nature of this project: "I can't remember the last time I had to write a cybersecurity article from scratch!"
- UCR: UCR is adopting the ISA Workgroup's year-round ISA program in its entirety.
- UCSD & UCSD Health: UCSD also adopted the entire ISA program, and is working with UCSD Health to deliver consistent messaging across campus and the health system.
- UCSB & UCLA: UCSB has launched a social media campaign utilizing materials from this project's toolkits. These platforms provide rich analytics that report engagement and monitor participation. UCLA IT Security also has an active presence on Twitter, which is a resource for the workgroup.
- Multiple locations:
    - Several UC locations regularly use the video shorts produced by UCSB and UCLA in video displays, social media, and online.
    - Several locations use and modify the posters and infographics from the various toolkits.
    - 10 UC locations registered with StaySafeOnline.org as National Cyber Security Awareness Month Champions, and 7 locations registered as Data Privacy Day Champions in 2017.
- Website: There are significant spikes in pageviews of the systemwide ISA homepage upon the announcement of a new ISA toolkit to ITPS.
- External: As mentioned above under "Impact," external requests to use our ISA materials are indicative of the perceived value of this project.

Systemwide Information Security Awareness Website:
Main page: https://security.ucop.edu/resources/security-awareness/index.html
Awareness campaigns: https://security.ucop.edu/resources/security-awareness/campaigns.html
Additional systemwide resources are available on the left side menu of these web pages.

BACKGROUND ON THE SYSTEMWIDE INFORMATION SECURITY AWARENESS WORKGROUP:

The ISA Workgroup is a collaboration across 12 UC locations (though it is open to all UC locations). The focus of this workgroup is on a strategic approach to ISA and related outreach; building good cybersecurity habits; and information and resource sharing. This includes, but is not limited to:

- Identifying strategies and common goals to promote good cybersecurity habits and campus ISA programs, as well as an improved cybersecurity posture systemwide.
- Creating and sharing resources used to promote campus-wide ISA program goals.
- Identifying and sharing cybersecurity themes for awareness activities.
- Reinforcing or expanding awareness messages from the UC SANS Cybersecurity Awareness Training.
- Identifying and sharing outreach methods and channels for awareness efforts, including ideas and strategies for how to use the materials and resources being developed and shared.
- Sharing lessons learned from awareness efforts, including what worked and what didn't, successes, ideas for improvement, etc.
- Participating in the broader ISA effort; being a good partner with other educational institutions and organizations.
- Developing measures of effectiveness to ensure our efforts, themes and materials have a relevant and valued impact on our UC customers.

SUPPLEMENTAL MATERIALS – Sample screenshots from the systemwide ISA website:

1) **Information Security Awareness Campaigns page** – links to current and past toolkits, plus NCSAM archives: https://security.ucop.edu/resources/security-awareness/campaigns.html

2) **Travel Cybersecurity Toolkit** – the most recent toolkit as-of May 2018: https://security.ucop.edu/resources/security-awareness/travel-cybersecurity-2018-campaign.html

Security Tips and Fact Sheets
Outreach Strategies
National Cyber Security Awareness Month Archive

SYSTEMWIDE INFORMATION SECURITY AWARENESS WORKGROUP CONTACTS

Davis	Dewight Kramer Maurice Anderson
Davis Health	IT Security email/internal website
Los Angeles	Security Awareness
Riverside	Bill Green 951-827-3072
San Diego	Ronise Zenon Matthew Bellino
San Diego Health	Marissa Ventura
San Francisco	Awareness Team
Santa Barbara	Awareness Team
Santa Cruz	Tamara Santos 831-459-2779
UC ANR	Tolgay Kizilelma David Hatter
Office of the President	Julie Goldstein Kamika Hughes

CAMPUS & UCOP INFORMATION SECURITY PROGRAMS

- Berkeley
- Davis
- Irvine & UC Irvine Health
- Los Angeles
- UCLA Health
- Merced
- Riverside
- San Diego
- San Diego Health System (login required)
- San Francisco & UCSF Medical Center
- Santa Barbara
- Santa Cruz
- Lawrence Berkeley National Lab
- Office of the President

Posters/Infographics**:

** 5 Online Security Tips for Smarter Travel

** Travel Securely from UCSC

Video Shorts:

- ** **TOP TIPS: Stay Safe While Traveling This Summer** – staysafeonline.org (1:45 min)
- Quick tips for online security while traveling -- STOP. THINK. CONNECT. (0:30 sec)
- Stay Secure While Traveling at Home and Abroad – UCLA IT Security (1:55 min)

Tipsheets:

- ** **Safety Tips for Mobile Devices** (1 page)
- ** **CyberTrip Advisor tip sheet** (downloads a 2-page PDF)
- Cybersecurity While Traveling Tip Card (2-page PDF)
- Safety and Security for the Business Professional Traveling Abroad (includes but is not limited to cybersecurity)
- Keep security in mind on your summer vacation (1 page)

Tweets from Educause:

- ** **Travel data light! The safest way to protect confidential data is to leave it at home.** #TravelSafe #CyberAware #PrivacyAware
- ** **Guard your devices! Set up tracking features & remote erasing options in case they're stolen.** #TravelSafe #CyberAware #PrivacyAware
- ** **Surf protected! Use a #VPN to stay connected & remember...free Wi-Fi isn't always secure.** #TravelSafe #CyberAware #PrivacyAware
- Pay attention! Set up alerts to monitor your online accounts when you're traveling #TravelSafe #CyberAware #PrivacyAware
- #Latergram! Wait until you return home to share all those beautiful vacation photos. #TravelSafe #CyberAware #PrivacyAware
- Additional tweets available at "Security Tips for Traveling at Home and Abroad" (scroll down to "Social Posts").

FTC Materials:

Printed materials from the Federal Trade Commission that you can order in bulk for free.
Laptop Security Tips bookmark

Additional Specialized Resources by Topic:

Inspection of electronic devices at the US border

- **UC website:** Traveling with Electronic Devices: briefly reviews the relevant law permitting border searches, describes key U.S. Customs and Border Patrol (CBP) policies relating to such searches, discusses frequently asked questions that UC faculty may have about their rights in connection with a border search, and general information about protecting sensitive data while traveling overseas on UC business.
- U.S. Customs and Border Protection's Inspection of Electronic Devices fact sheet
  - Full CBP "Border Search of Electronic Devices" Directive, Jan 2018 (12 pages)
- Detailed guidance and analysis from eff.org (52 pages): Digital Privacy at the U.S. Border: Protecting the Data On Your Devices

International Compliance and Export Control

- UC Ethics, Compliance and Audit Services (ECAS) "International Compliance" site. Includes:
  - Updated guidance in ECAS' April 2018 Compliance Alert newsletter (see "International Compliance" on pg 3)
  - International travel
  - Hand-carrying items abroad
  - Export control information, including export of technology
  - Webinar: Top 10 Things You MUST Know before Taking Your Laptop Overseas (Brian Warshawsky, from 2013) *slides only*
  - More...

UC Global Operations (UC GO) website

A broad range of information for UC faculty, researchers, staff, administration, students, trainees, and international students and scholars traveling internationally. Most content is not technology or privacy related. Related to cybersecurity, includes

- Laptop and data security
- Export controls

Resources from the Higher Ed Community

Large compilation of web pages from Higher Ed, government and related communities with security tips and information for traveling abroad - from Educause/Internet2

UNIVERSITY OF CALIFORNIA UCOP.EDU
