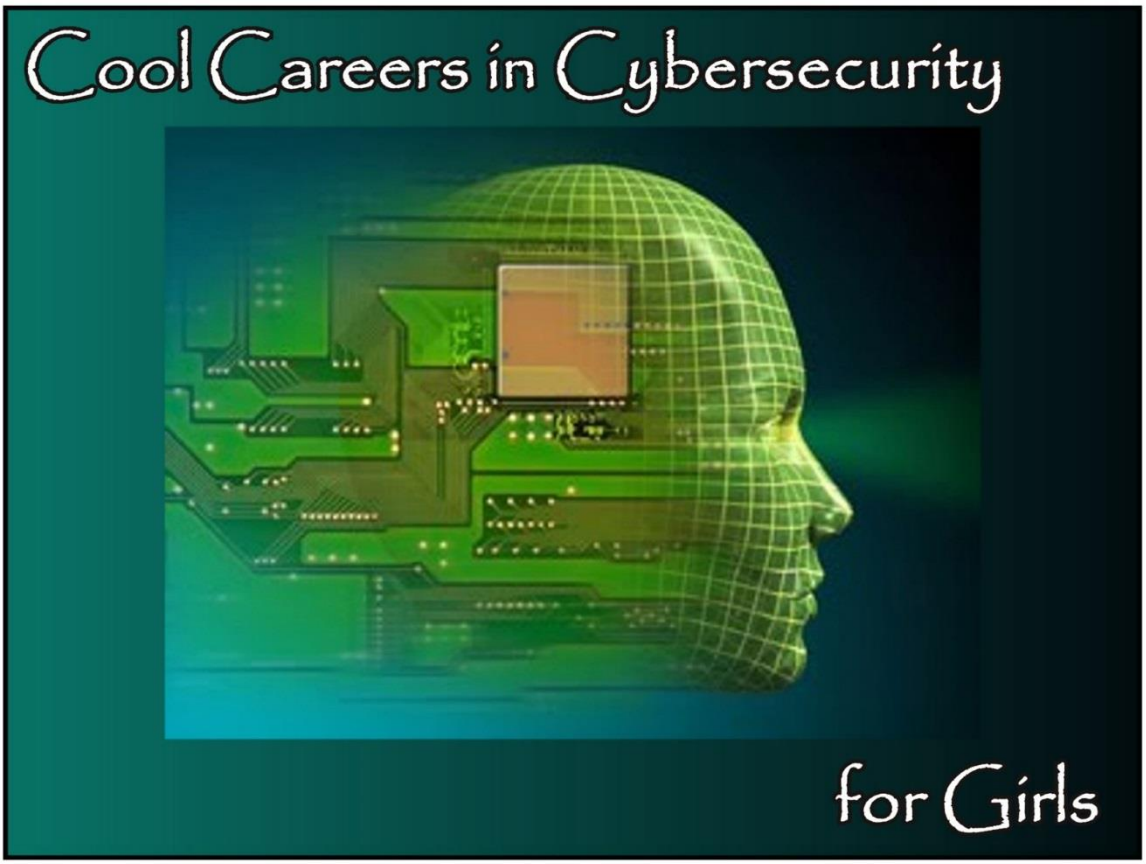
ETPRO

MARYLAND CYBERSECURITY CENTER

national CyberWatch center

Info Security Crime Investigator • Malware Analyst • Incident Responder • Forensic Analyst

Security Architect • Penetration Tester • Network Security Engineer



Vulnerability Researcher • Exploit Developer • Security Auditor

Computer Crime Investigator • Security Operations Center Analyst • Intrusion Analyst

MARYLAND CENTER FOR WOMEN IN COMPUTING

NSF

Cool Careers in Cybersecurity for Girls Workshop C34G

November 12, 2014
10 a.m. to 1:00 p.m.
Riggs Alumni Center at the
University of Maryland - College Park, MD

Cool Careers in Cybersecurity for Girls (C34G) educates, inspires, and provides girls with the information, skills and resources necessary to navigate the professional pipeline in the vast field of cybersecurity. Our vision is put into action through programs and a focus on cyber stewardship, activities to make a safer and more secure society, by delivering high-quality, innovative activities that inspire girls to pursue careers in cybersecurity.

The National CyberWatch Center K-12 Division, led by Educational Technology Policy, Research and Outreach, in partnership with the University of Maryland is excited to partner with the University of Maryland to offer another outstanding Cool Careers in Cyber Security for Girls Workshop at the University of Maryland, College Park Campus. The event would not be possible without women professionals volunteering their time. We would like to thank the women from the following organizations who volunteered their time to help middle school girls understand how their innate gifts and interests can help them have a successful career in any STEM field.

- Boeing
- Howard Community College
- Lockheed Martin
- National Security Agency (NSA)
- Northrop Grumman
- Northrop Grumman WiNGs
- Schnell-Tech Solutions
- Tenable
- University of Maryland College Park -OIT
- University of Maryland University College (UMUC)
- U.S. Department of Agriculture
- U.S. Department of Education

Thank you once again for your time and commitment to this event.

Speaker Guide

The National CyberWatch Center K-12 Division, led by Educational Technology Policy, Research and Outreach, in partnership with the University of Maryland thanks you for volunteering to present at the Cool Careers in Cybersecurity for Girls Workshop. We could not do this without your willingness to share your experiences with our middle school girls.

This speaker guide will help you prepare for the day and assist you in answering student questions. It contains:

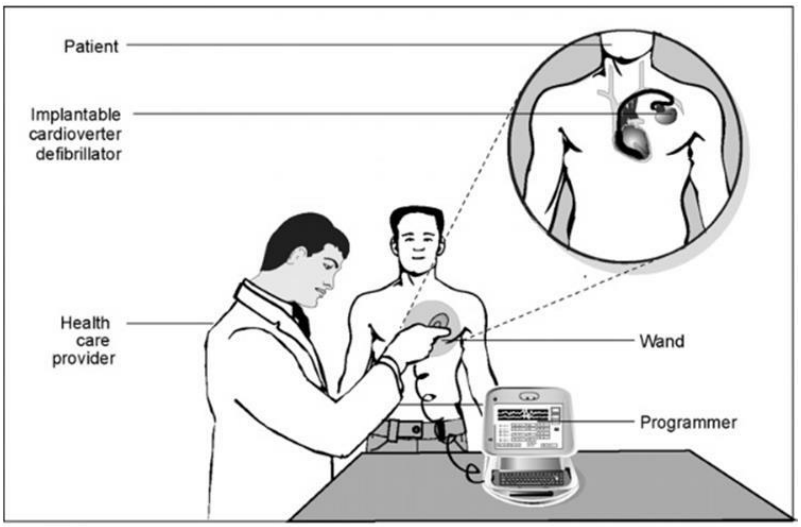
- Scenario
- Agenda
- Annotated Agenda with additional ideas on ways you can help the event go smoothly
- Activities and clues (in case you are curious about the crime)
- Questions students have asked Women STEM Professionals about Cybersecurity in the past
- Directions and parking information

Scenario

Middle school girls become Cyber Super-Investigators (CSI) for a day to solve a cyber-crime.

During this interactive crime solving event, girls learn from women in diverse companies and agencies about what it takes to navigate the professional pipeline in the vast fields of Cybersecurity and Information Assurance, as well as other science, technology, engineering, and mathematics (STEM) fields.

The middle school girls complete hands-on activities with guidance from cybersecurity and STEM professionals in order to gather clues to help solve the crime. This year's cybercrime scenario focuses on vulnerabilities in networked medical equipment.



Source: GAO.

On an episode of the *Showtime* series *Homeland,* Vice President Walden's pacemaker was hacked becoming the weapon for his assassination. In a *60 Minutes* interview with former Vice President Dick Cheney, he confirmed that the possibility of his pacemaker being hacked had been discussed and the device's wireless access had been disabled to prevent such an attack on his life.

Although it may sound like science fiction several studies have proven that flaws in cyber security of medical devices could be exploited to induce death.

- Computer scientist Kevin Fu has demonstrated in a research lab that he could hack into a combination heart defibrillator and pacemaker to induce potentially fatal electric jolts.
- Researchers at computer security firm McAfee share they have found a way to hack into an insulin pump to make it release multiple days worth of insulin.
- Security analysts Terry McCorkle and Billy Rios discovered a simple password vulnerability affecting over 300 devices including ventilators, drug infusion pumps, external defibrillators, patient monitors, and laboratory and analysis equipment. Devices could be exploited to change critical settings or modify the device.

In the case of our scenario, the 2014 Cool Careers Cyber Crime: *Networked Medical Equipment Vulnerabilities*, the all girls' middle school Cyber Super-Investigators (CSI) have been hired to examine in greater detail how medical devices could be breached and make recommendations to the U.S. Food and Drug Administration.

The girls will collect and explore a variety of digital and physical evidence to learn more about medical device vulnerabilities. Clues provided by the lead investigators, the cyber professionals speaking at the Cool Careers in Cybersecurity for Girls Workshop, will help the middle school girls in their investigation!

Related Content

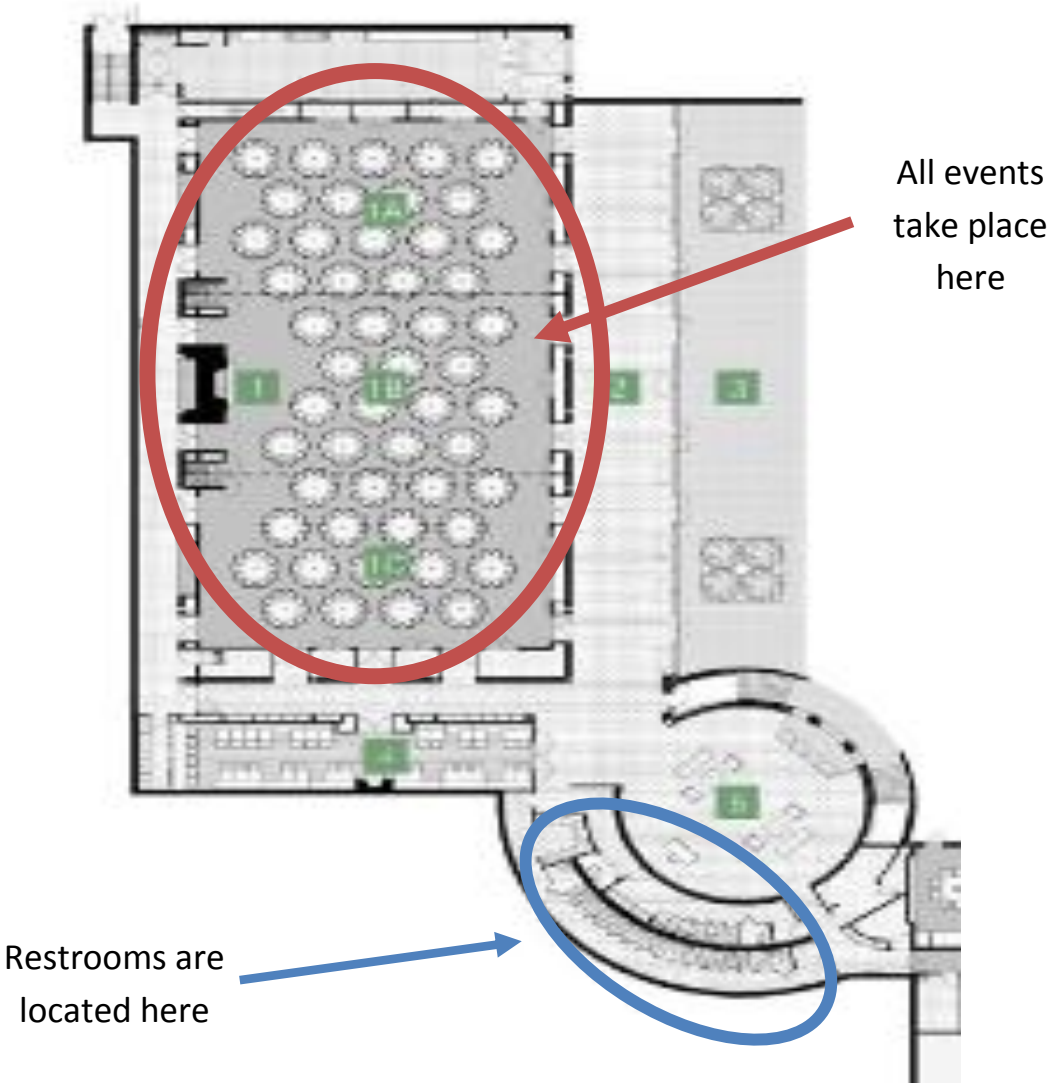
Some of the reports indicate some rudimentary causes for medical equipment breaches; some from known software flaws, and others from end-user related vulnerabilities including:

- Lack of authentication to access or manipulate the equipment
    - Table activity: Physical security and lock picking
    - Table activity: Find the USB drives
- Weak passwords set by users as well as weak or default hard-coded passwords set by the vendor – passwords like “1234” and “admin”
    - Table activity: Cryptography
    - Table activity: Password strength
- Using very old versions of Windows that are susceptible to viruses from years ago. Hospitals have to use the older systems because some manufacturers will not allow their equipment to be modified with the newer versions, partially due to regulatory restrictions.
    - Table activity: Computer anatomy
- Embedded web servers and administrative interfaces that make devices obvious and vulnerable to a breach within the network
    - Wi-Fi network attacks

AGENDA

9:15 am	Speakers arrive
9:30 am	Arrival Meet the CyberCareer Speakers
10:00-10:05 am	Welcome and Introductions Dr. Davina Pruitt-Mentle Dr. Michel Cukier
10:05 - 10:20 am	Setting the stage for scenario and activities/Video
10:20 - 10:40 am	Activity 1/ Rotation 1
10:43 - 11:03 am	Activity 2/ Rotation 2
11:05 - 11:25 am	Activity 3/ Rotation 3
11:27– 11:50 am	Activity 4/ Rotation 4
11:50 – 12:15 pm	Organize at Lunch Tables
12:15 – 12:35 pm	Activity 5 Lunch Keynote Speaker: Panel Session
12:35-1:00 pm	Activity 6 Discussion of the CyberCrime, Thank You's and Evaluations

If you should find a lost student this will help you direct her.



Agenda with Notes

9:15 a.m.	Speakers arrive	We ask that speakers arrive on or before 9:15 a.m. You will check in at the registration desk and will be directed to your table. After reviewing the materials you should have time to grab some coffee and a danish that we will provide.
Arrival – 9:30 a.m.	Meet Cyber Career Speakers	Buses are scheduled to arrive between 9:30 and 9:45 a.m. I**t would be great if speakers could make themselves available to talk to students who arrive before 9:45.** Quotes about why our speakers say their careers are cool will be shown throughout the room. Speakers can walk around the room or stay close to their assigned table. We will encourage students to take advantage of this time to introduce themselves to the speakers and ask a few questions. We will have coffee and refreshments for presenters in the AM The restrooms are indicated in the above map. **Speakers can help usher students toward the appropriate tables**. Students must be in their seats by 9:55 so that we can begin on time. Students are asked to stay at their assigned tables and rotate as a group as detailed in the schedule.
10:00 - 10:05 a.m.	Welcome and Introductions	Students will be welcomed and the organizations which have supported us with speakers will be introduced. Welcome and Introductions: Dr. Davina Pruitt-Mentle
10:05 - 10:20 a.m.	Setting the stage for scenario and activities/video	Logistics will be covered about how the day will proceed. An introductory video will be shown to set the stage for the cybercrime students will be asked to explore.

10:20 - 10:40.	Activity 1	Students will be pre-assigned starting tables and will rotate as a group as detailed in the schedule. **We have allowed 5 minutes between rotations; however, you are welcome to begin as soon as all ladies are seated and ready to begin.** **During the Activity 4 please thank students for being so polite and cooperative up to this point and remind them that there is still more to come.**
10:43 - 11:03	Activity 2	
11:05 - 11:25	Activity 3	
11:27– 11:50	Activity 4	
11:50- 12:15	Organize at Lunch Tables	Groups will stay at the Activity 4 table for the luncheon speaker and lunch. Teachers and volunteers will be bringing the box lunches to the tables. Along with parents, chaperones and teachers, we ask speakers to remind students to “unwrap” their lunches as soon as possible so that noise is limited during the keynote speaker presentation. The lunchtime speaker is going to begin promptly at 12:20 so the students need to be in their seats, quiet and ready to pay attention. Setting the expectation after this last session will help us stay on schedule. No one is allowed to enter or leave the room during the keynote speaker session.
12:15- 12:35	Activity 5	Dr. Michel Cukier Introduction + Lunch Keynote Speaker Panel Session
12:35- 1:00	Activity 6	Dr. Davina Pruitt-Mentle, Closure Solve the Cyber Crime, Q and A, Thank You’s and Evaluations
1:00	Depart	Load Buses

This table lists the Table each presenter is assigned and the groups that each will interact with for each rotation.

Table	Presenter, Organization, Topic, Activity	START & Rotation 1	Rotation 2	Rotation 3	Rotation4
1	Vonda Williams, Computer Parts Dr. Monica Brodzik, NSA	Harpers 1	Hyatt 3	Lake Elkhorn 4	St Louis 5 and Indiv A
2	Lolli Buran, LMC Computer Parts	Harpers 2	Hyatt 4	Lake Elkhorn 5	Clarksville 1
3	Lisa McKelvie Ms. Elise Campbell, NSA Computer Parts	Harpers 3	Hyatt 5	Gaithers 1	Clarksville 2
4	Cyndi Gula, Tenable Computer Parts	Harpers 4	Thomas P 1	Gaithers 2	Clarksville 3
5	Angela Pompey, USDA Computer Parts	Harpers 5	Thomas P 2	Gaithers 3	Clarksville 4
6	Emma Garrison, UMUC Computer Parts	St Louis 1	Thomas P 3	Gaithers 4	Clarksville 5
7	Kelly O'Brien, LMC Computer Parts	St Louis 2	Thomas P 4	Gaithers 5	Lake Elkhorn 1
8	Stacey Hertz, LMC Computer Parts	St Louis 3	Thomas P 5	Hyatt 1	Lake Elkhorn 2
9	Pamela Mitchell, HCC Computer Parts	St Louis 4	Bullis	Hyatt 2	Lake Elkhorn 3
10	Kristen Lantz, LMC USB Drives	St Louis 5 and Indiv A	Harpers 1	Hyatt 3	Lake Elkhorn 4
11	Mary Phillips, LMC USB Drives	Clarksville 1	Harpers 2	Hyatt 4	Lake Elkhorn 5
12	Amy Ginther, UMD-OIT USB Drives	Clarksville 2	Harpers 3	Hyatt 5	Gaithers 1
13	Colleen Calimer, Boeing USB Drives	Clarksville 3	Harpers 4	Thomas P 1	Gaithers 2
14	Angela Scott, LMC USB Drives	Clarksville 4	Harpers 5	Thomas P 2	Gaithers 3
15	Alice Chang, Tenable Katie Hirsch, Tenable USB Drives	Clarksville 5	St Louis 1	Thomas P 3	Gaithers 4
16	Phyllis King, NGC WiNGS Kelly Soverns, NGC WiNGS USB Drives	Lake Elkhorn 1	St Louis 2	Thomas P 4	Gaithers 5
17	Moira Parham, Tenable USB Drives	Lake Elkhorn 2	St Louis 3	Thomas P 5	Hyatt 1

18	Rozaliya Volynskiy, HCC USB Drives	Lake Elkhorn 3	St Louis 4	Bullis	Hyatt 2
19	Caryn Boyd, DoEd Lock Picking	Lake Elkhorn 4	St Louis 5 and Indiv A	Harpers 1	Hyatt 3
20	Sharon Washington, DoEd Lock Picking	Lake Elkhorn 5	Clarksville 1	Harpers 2	Hyatt 4
21	Katrina Raysor, DoEd Lock Picking	Gaithers 1	Clarksville 2	Harpers 3	Hyatt 5
22	Gail Schnell, Schnell-Tech Solutions Zen Jones Lock Picking	Gaithers 2	Clarksville 3	Harpers 4	Thomas P 1
23	Karen Edwards, DoEd Lock Picking	Gaithers 3	Clarksville 4	Harpers 5	Thomas P 2
24	Harriette Julian, NGC WiNGs Heather Thomas, NSA Lock Picking	Gaithers 4	Clarksville 5	St Louis 1	Thomas P 3
25	Rosemary Shumba, UMUC Lock Picking	Gaithers 5	Lake Elkhorn 1	St Louis 2	Thomas P 4
26	Laura Hobbs, Tenable Lock Picking	Hyatt 1	Lake Elkhorn 2	St Louis 3	Thomas P 5
27	Alice Shaffer, NSA Lock Picking	Hyatt 2	Lake Elkhorn 3	St Louis 4	Bullis
28	Dr. Laurel Boraz, NSA Crypto	Hyatt 3	Lake Elkhorn 4	St Louis 5 and Indiv A	Harpers 1
29	Valerie Boykin, DoEd Bria Flowers, NSA Crypto	Hyatt 4	Lake Elkhorn 5	Clarksville 1	Harpers 2
30	Pamela Lougee, NSA Gail Briemann, NSA Crypto	Hyatt 5	Gaithers 1	Clarksville 2	Harpers 3
31	Dawn Beyer, LMC Crypto	Thomas P 1	Gaithers 2	Clarksville 3	Harpers 4
32	Bernadette Bucher, LMC Crypto	Thomas P 2	Gaithers 3	Clarksville 4	Harpers 5
33	Anh Tran, LMC Crypto	Thomas P 3	Gaithers 4	Clarksville 5	St Louis 1
34	Jacquelyn Blanchard, LMC Crypto	Thomas P 4	Gaithers 5	Lake Elkhorn 1	St Louis 2
35	Ebony Pierce, LMC Crypto	Thomas P 5	Hyatt 1	Lake Elkhorn 2	St Louis 3
36	Rebecca Robley, NSA Crypto	Bullis	Hyatt 2	Lake Elkhorn 3	St Louis 4
37		6 PG students: journalism task			

This table lists the starting position and rotations for each of the schools

WHO	Abbreviation/Group # Number of students/chaperones	START & Activity 1	Activity 2	Activity3	Activity 4 & Stay for lunch
		TABLE	TABLE	TABLE	TABLE
Clarksville 1	Clarksville 1 8 students/ 1 chap	11	20	29	2
Clarksville 2	Clarksville 2 8 students	12	21	30	3
Clarksville 3	Clarksville 3 8 students/ 1 chap	13	22	31	4
Clarksville 4	Clarksville 4 8 students	14	23	32	5
Clarksville 5	Clarksville 5 8 students/ 1 chap	15	24	33	6
St Louis 1	St Louis 1 8 students/ 1 chap	6	15	24	33
St Louis 2	St Louis 2 8 students	7	16	25	34
St Louis 3	St Louis 3 8 students/ 1 chap	8	17	26	35
St Louis 4	St Louis 4 8 students	9	18	27	36
St Louis 5 & Indiv A	St Louis 5 4 students + 4 Indiv A	10	19	28	1
Gaithersburg 1	Gaithersburg 1 8 students/ 1 chap	21	30	3	12
Gaithersburg 2	Gaithersburg 2 8 students/ 1 chap	22	31	4	13
Gaithersburg 3	Gaithersburg 3 8 students/ 1 chap	23	32	5	14
Gaithersburg 4	Gaithersburg 4 8 students/ 1 chap	24	33	6	15
Gaithersburg 5	Gaithersburg 5 8 students/ 1 chap	25	34	7	16
Lake Elkhorn 1	Lake Elkhorn 1 8 students/ 1 chap	16	25	34	7
Lake Elkhorn 2	Lake Elkhorn 2 8 students/ 1 chap	17	26	35	8
Lake Elkhorn 3	Lake Elkhorn 3 8 students/ 1 chap	18	27	36	9
Lake Elkhorn 4	Lake Elkhorn 4 8 students/ 1 chap	19	28	1	10
Lake Elkhorn 5	Lake Elkhorn 5 8 students/ 1 chap	20	29	2	11
Hyattsville 1	Hyattsville 1 8 students/ 1 chap	26	35	8	17
Hyattsville 2	Hyattsville 2	27	36	9	18

	8 students				
Hyattsville 3	Hyattsville 3 8 students/ 1 chap	28	1	10	19
Hyattsville 4	Hyattsville 4 8 students/ 1 chap	29	2	11	20
Hyattsville 5	Hyattsville 15 8 students/ 1 chap	30	3	12	21
Harpers Choice1	Harpers 1 8 students/ 1 chap	1	10	19	28
Harpers Choice2	Harpers 2 8 students	2	11	20	29
Harpers Choice3	Harpers 3 8 students/ 1 chap	3	12	21	30
Harpers Choice4	Harpers 4 8 students/ 1 chap	4	13	22	31
Harpers Choice5	Harpers 5 8 students/ 1 chap	5	14	23	32
Thomas Pullen 1	Thomas Pullen 1 8 students/ 1 chap	31	4	13	22
Thomas Pullen 2	Thomas Pullen 2 8 students/ 1 chap	32	5	14	23
Thomas Pullen 3	Thomas Pullen 3 8 students/ 1 chap	33	6	15	24
Thomas Pullen 4	Thomas Pullen 4 8 students/ 1 chap	34	7	16	25
Thomas Pullen 5	Thomas Pullen 5 8 students/ 1 chap	35	8	17	26
Bullis	9 Students/2 chap	36	9	18	27
Student reporters	6 students and other PG staff	37			

SCHOOL	District	School Teacher Lead
Bullis	Private	Rita Gerharz
Clarksville	Howard	Philip Herdman
Gaithersburg	Montgomery	Michael Ryan
Harpers Choice (HC)	Howard	Adam Eldridge
Hyattsville	Prince George's	Ronnie Lowenstein
Lake Elkhorn	Howard	David Bond
St Louis Catholic School (SL)	Archdiocese of Baltimore	Zulma Whiteford
Thomas Pullen CPA	Prince George's	Ronnie Lowenstein
Individual A	NA	Individual Contacts to Attend

Activities and Clues: Just in case you are curious about possible clues to the crime

Topic	Clue	Activity
Physical Security	Physical security is important! Being able to access a room makes it a lot easier to manipulate equipment, medical records, or other electronic devices. Even things locked with a padlock can be accessed. How easy is it to pick a lock or guess a combination? What recommendations does the team have for physical security access?	Lock Picking
Cryptography	Once the serial and model numbers of the pacemaker are known, someone could then reprogram the firmware of a transmitter, which would allow reprogramming of a pacemaker in a person's body. An encrypted message was sent with important information. Can you break the code? What recommendations does the team have for more secure codes?	Frequency Chart and Cipher
Steganography	Several pictures are presented. Which picture contains hidden information? How can you tell? Could you have detected the hidden message without the cryptographic instructions? How could you protect against this type of threat?	Which picture has the files?
Digital Forensics 1	What are potential ways for thieves to steal or copy important information? Today many companies do not allow electronic or storage devices to be taken into work. Several organizations/companies actually inspect coats, bags, and briefcases to make sure the policy is followed. Hidden USB drives can be planted in women's jewelry bag and/or brief cases. Can you find all the hidden storage devices? What recommendations would you suggest to protect against the threat of removable media such as thumb drives?	Find the USB drives
Computer Science 1	Evidence was found on the thief's work computers. The team will examine computers used by the medical staff to control the medical device. The team will want to make sure that the problem did not originate with the original instructions given to the medical device by the medical practitioner. Alternatively, they will want to examine if a malicious set of instructions were entered. However, they have been disassembled. Further investigation reveals parts are missing. What parts were missing? A key part of being a cyber investigator is not only seeing what is there, but also noticing what is missing.	Find the missing parts
Computer Science 2	Evidence was found on the suspect's home computer. However, the keyboard is missing. Is there another way to use the computer without a keyboard?	Makey Makey
Digital Forensics 2	Clues can be gathered by exploring the suspect's browser history and cookies. Although these can be deleted, luckily the cybercriminal was not that smart. See if you can find anything related to the crime in the history and cookies. Make sure to look at all browsers on the system. How could the thief have avoided leaving this information behind?	Browser History
Social Engineering	How did the thief get access to some of the files? In many cases, high tech gadgets and knowledge is not even needed. Tactics such as social engineering can be used to gather incredible amounts of information. Spoofing or disguising the caller's number and even their voice make these tactics even easier. Can you protect against the types of attacks we demonstrated?	Spoofing

Questions Students have asked about Cyber Security and Women STEM Professionals in the past

Students have asked these questions in the past. You may want to think about how you would answer these questions if asked.

Cybersecurity careers

- How is cybersecurity used in today's jobs? How does cybersecurity affect other jobs?
- What types of jobs are cybersecurity jobs?
- What are the job responsibilities in each of the cybersecurity fields?
- How many hours a day do cybersecurity employees work?
- How much do cybersecurity workers get paid?
- What kind of people do cybersecurity professionals work with?
- What courses should I take if I am interested in this field?

Connection of information assurance to other careers

- How does cybersecurity protect us?
- How will knowing about cybersecurity help me with my career?
- How can I become more familiar with how computers work?

Hackers

- How do you become a hacker? What do you need to know?
- What do hackers know? What do hackers do? What do hackers want from me?

Security of personal data and computers

- How are we protected on the internet?
- How do you keep information safe on the internet?
- How do the various computer programs work to protect my information?
- How do I protect my computer and information?
- How safe is my computer now?
- How do I get rid of viruses?

Women STEM Professionals

- What do you wear to work?
- Do you have a family? Is it hard to work and have a family?
- What benefits does your company offer?
- Do you travel?
- What hours do you work?
- How many women do you work with?

Directions

The Samuel Riggs IV Alumni Center is on the University of Maryland College Park Campus http://www.riggs.umd.edu/

The Samuel Riggs IV Alumni Center does not have a physical address. If you would like directions to the facility from your starting address, please go to http://riggs.umd.edu/map.html

THE SAMUEL RIGGS IV ALUMNI CENTER is situated on the University of Maryland, College Park campus—conveniently located off of I-495 and close to the College Park Metro Station. The center is at the hub of the university's northwest corner next to the Clarice Smith Performing Arts Center and Byrd Stadium. I would suggest (if coming off 95) exit onto Route 1 towards College Park. Exit onto Route 193. At the second traffic light, take a left onto Stadium Drive. Enter the round about—bear off first right (stadium Garage is on the left and so is the Riggs Alumni Center. If you get to a second round about—you've gone too far.

Parking is available in the Stadium Parking garage next to the Riggs Alumni Center. Cost is $3.00 /hr or $15.00 for the full day. You will park, remember you're parking # and pay at the parking booth. Please bring the receipt and turn it in to us with your full name, address and phone number printed on the back of receipt (or we will have forms to complete).