Quarterly Cybersecurity BILT Meeting October 10, 2012
Meeting Minutes

Trends

Stephen Miller: Scada systems: cybersecurity but physical security does tie in a little bit, is part of risk assessment.

Erich Spengler: From a two year technician stand point should we be focusing on risk, is that disaster recovery area.

Stephen Miller: We just cover physical control in our curriculum just not in that depth.

Caroline Dennis: This speaks to the KSA; hardware hacking and understanding how it works is a trigger point for the private industry. The bigger firms who do the forensics they are looking for the engineering but are looking for more. With chips being made in china will become a bigger focus. Having students know how the chips were made and the languages would be good.

Jared Sutton: In a survey class, but the model of chips would be more than a 2 year degree, since there are some many different types of chips.

Erich Spengler: We do have a full blown class that does exactly what you just said so I am very glad you just said that.

Caroline Dennis: This would make someone a very viable candidate.

Labor Market

Ann Beheler: What do you see in terms of labor market demands for a specialty in security? What kind of jobs would be appropriate for 2 yr grads: what does hiring look like? What are the right skilled people?

Mark Leech City of Albuquerque: Increase in this of data privacy, it's interesting and being forced on us but there are several positions we are looking at.

Stephen Miller: I have been working with homeland security and veteran administration: military people getting out could take this cybersecurity could get an information technology degree, quite a few in DC. Starting at 55,000. It's key to have some of the curriculum certified. Cyber security specialist. Has a list of 20 cybersecurity jobs. Will send all the research he has done. Had a 16% increase in the number of cyber security jobs. Also the DOL just this year set up a category for Information systems analyst.

Alan Greenburg: He also sees a two year trends for non DOD realms home depot has 15 cybersecurity positions.

Stephen Miller: We are trying to get the federal government to hire people with two year degree minimum. Dr. McDuffy from the NIST. There are jobs out there for two year grads, hard part is getting people to realize they are very good to hire.

Caroline Dennis: The private industry working under the chief security officer there are defiantly two year jobs. Managed services is the proactive patching services, is the third party company that large companies pay to do for them. Those companies entail the perfect place for an entry level employee. Training, many of the larger security companies have a training department who train clients and there are positions for them there as well.

KSAs

Ann Beheler: Typically this process works by identifying 2.5 or higher as items that we include in our curriculum. First I would like to look at those identified below 2.5.

Ann Beheler: Know of remote access technology concepts and Knowledge of server administration and systems engineering theories, concepts, and methods both 2.3.

Stephen Miller: It's good to cover it somewhat remote access will be covered in security awareness. Should be covered in the curriculum.

Caroline Dennis: Not sure which way you are looking at this, it is important.

Stephen Miller: Mapping course content to Info Sec 4011 on these two topics.

Erich Spengler: I think that it's an important function.

Ann Beheler: Sometimes people rank low because some people think that the highest number means perfect. So what I am hearing is that we need to cover this.

Caroline Dennis: At least the first one it is very critical

Stephen Miller: If you're going to map the Info Sec 4011 then the question is how much in depth are you going to cover it? Not that much it is covered in several courses.

Erich Spengler: There are three areas task, knowledge, and skills.

Mark Leech: They might have been low, because they are needed but they are woven into everything else, having knowledge about administration would be picked up in all courses.

Ann Beheler: Moving to the top, sorry for getting confused. Can we move to task, new or observed threats of an enterprise ranked 2.4.

Caroline Dennis: May ask the question of how in-depth one can get in 2 yrs? Signatures are a very hot topic.

Jared Sutton: It was rated low because a year 2 wouldn't be constructing these signatures they would be pushing them out.

Ann Beheler: So more of an awareness then?

Jared Sutton: Yes, the 2 yrs would be the first to know of a signature attack and how to fix it, but they will not be constructing them.

Ann Beheler: Knowledge of domain guards 2.3. What if we leave that out is it ok or does it matter?

It's awareness.

Erich Spengler: I am going to have to research that a little more.

Caroline Dennis: look at the ability to automatically or manually transfer information between two domains.

Erich Spengler: It is more for a higher level.

Caroline Dennis: I would agree it's a higher level.

Ann Beheler: 2.3 maintaining information exchanges through published etc. cover it don't cover it cover it lightly? We pulled it from nice.

Caroline Dennis: I think this is huge especially in the job of forensic, they do a lot of data monitoring and they would deal with it.

Erich Spengler: What jumps to my mind something on the user level, how do you securely exchange information through domains. A lot of people do secure HDP, exchanging information securely. Even knowledge of a VPN would be included.

Ann Beheler: Knowledge of agency Lan Wan pathways.

Erich Spengler: Routing, could even include firewall

Stephen Miller: Cover it.

Caroline Dennis: Can you speak to how much foundational networking a student should have before they go into cybersecurity.

Erich Spengler: How we approach it with stackable, we have a core that is equivalent to a CCNA base some classes can be taken at the same time. They take security + then they can move up to higher commodity learning.

Stephen Miller: That is how our source is laid out; you would take a COMPTIA and then move up.

Erich Spengler: Correct ethical hacking, and the CCNA hardware. So what's the base, since security is such a commodity skills?

Caroline Dennis: I wouldn't want too many core, it sounds like they can take forensics while working on their.

Jared Sutton: More of a database, not sure it needs to be covered.

Ann Beheler: Enterprise message programs 2.3, important of not

Jared Sutton: I think it came down to what job title we are looking at

Caroline Dennis: What are the other job titles?

Ann Beheler: Erich Spengler you might want to give a background on where the KSA came from.

Erich Spengler: With cybersecurity there are so many KSAs out there, for us teach we need a bench mark, so what we turned from nice nit framework, pulled from what we felt best fit.

John Sands: What you need to understand that the NIST framework is they took this over for the government; this NICE frame work is that they will be a clearing house for everything.

Erich Spengler: So the NIST- NICE framework allows us to, determine the controls from NIST to certify information.

Stephen Miller: That is what the workshop I talked about is tied into, that NICE framework.

Ann Beheler: Knowledge of network and access.

Caroline Dennis: Very important, even having a real core and understanding of that is very important.

Ann Beheler: Knowledge of telecommunication concepts.

Stephen Miller: Information to know but not critical.

Ann Beheler: Probably would be covered in our networking course.

Digital forensics

Ann Beheler: Decrypt seize data means:

John Sands: I would say that is pretty critical skills

Jared Sutton: I think this one unbelievably vague, if it means someone of a crypt.

Caroline Dennis: Knowledge of ability and skills, it's a Pandora's Box it can be simple or complicated.

Jared Sutton: A two year person should know what the different types and methods for encryption are.

Ann Beheler: Perform Tier 1, Tier 2, and Tier 3 malware analysis.

Caroline Dennis: Probably rated low because it's more than a two year.

Jared Sutton: What you would want a two year to know is covered in other areas, handling data, getting data ready. Anything more than that would be too advanced.

Ann Beheler: Using malicious code. Keep it static not dynamic.

Caroline Dennis: Does not agree that would not be hard to do in lab, that is a critical part of cyber jobs, at least a monitor job.

John Sands: Many of those tools are designed so that you don't have to be a specialist to use.

Paula Velluto: In our forensics program we do this in our security courses. Because, in forensic it tends to be static.

Stephen Miller: That's how we do it too.

Caroline Dennis: I will get back to you on this I want to talk to those in recruiting on this.

Stephen Miller: From a digital forensic are we saying this is not as important?

Caroline Dennis: I think that to be able to see how things are moving, to look at and to monitor and to interpret data, I think its higher up there, I want to talk to someone I would ask to verify that.

Stephen Miller: Absolutely.

Ann Beheler: Knowledge of security event correlation tools.

Caroline Dennis: Similar bucket.

Ann Beheler: Do you want to ask about that one to?

Caroline Dennis: If that was an event and it already happened then it should be important.

Paula Velluto: We have this in our security. At Umass this is where this would hit, they have full courses on this we have moved higher forensics to the 4 year level. They might be exposed at the 2 year.

Stephen Miller: We said this would probably be more of a senior level, although, I have taught entry level so that you do not cross legal levels.

Caroline Dennis: Maybe this is a knowledge base of imaging, it doesn't have to be in huge depth, but you should know what to do with a database.

Paula Velluto: This is about testifying.

Stephen Miller: We have dedicated a whole lab where they have put all the data and the forensics in a specific portfolio so that when and if they had to testify then the data is ready.

Paula Velluto: Our students in their last semester have to do a mock testify. At the two year level.

Caroline Dennis: That is fabulous.

Jared Sutton: I think the reason it came in at that low number is that most of the people in the room thought that someone at a 2 yr level would never testify.

Ann Beheler: Incident response.

Ranked at 1.7; probably because they would want a higher ranked person.

Caroline Dennis: Does speak to a broad thing to speak to police. I think there is a more general piece here. Do we want an entry level person speak to police if they don't have to.

Split to provide guidance and support to senior person

Stephen Miller: A senior person would do that, but they should have some awareness on this. So they are aware of the process, they will not most likely be doing this as a 2 yr graduate.

Ann Beheler: Knowledge of defense security implementation guides.

Caroline Dennis: Think is it very specific, if this is agency specific.

Stephen Miller: They will train them specifically will not be something we have in a course we will not be in that likely specific.

Network services

Ann Beheler: Remote you already said you wanted them to have it. Knowledge of capabilities of different electronic devices;

John Sands: I don't understand that one either; it is a fundamental one that we already cover in networking.

Jared Sutton: It's another one of that they are so woven into the other courses.

Ann Beheler: We are taking this to compare it to current curriculum to make changes to it.

Erich Spengler: We have Security Awareness, Security +, Ethical hacking, Linux course, 2 network security CCNA and a capstone course. Basic network forensic course, also looking into an advanced forensic that deals with mobile devices.