Using the Cyber-CHAMP Model to Determine Cyber Competencies and Role Alignment

August 2021

Team SS Cyberian

Abigail Moody, University of Idaho

Andrew Killpack, Brigham Young University - Idaho

Autumn Clark, Idaho State University

Jason Forbush, Idaho State University

Kyler Combe, Idaho State University

Thomas Upchurch, College of Southern Idaho

INL Mentor

Shane Stailey

Abstract

Cybersecurity roles, tasks, and skills are seen by many organizations as nonessential, abstract, or complicated. Although standards are in place, such as the National Institute of Standards and Technology (NIST) 800-181 document titled “Workforce Framework for Cybersecurity (NICE Framework)” available since September 2012, companies are still showing security vulnerabilities in their cyber networks (Hatzes, 2020). Barriers towards creating a cyber-ready workforce are not always due to a lack of resources, but often caused by organizational structure. The need for cyber-cognizant job postings, improved communication between Operational Technology (OT) and Information Technology (IT) employees, increases in staffing and funding for cyber teams, and better communication of standards and training can all contribute to increasing an organization’s cyber resilience. Cybersecurity Competency Health and Maturity Progression model (CYBER-CHAMP) is a model aimed at evaluating an organization’s structure and individual employee’s cyber knowledge and helps develop a plan to reach competency. This model was used to engage with organizations to promote proper cyber protocols and policies. The aim of this paper is to answer if it is possible for an organization to build a cyber-ready workforce by providing education and training options for current employees and prepare the future workforce to be ready on day one of employment. Both open source and firsthand interviews with organizations were used to conduct the research contained in this document. Further research may include additional development to the CYBER-CHAMP model and its delivery platform.

ICRP

Introduction

Although the need for cybersecurity has been a reality for decades, is still a new concept for many organizations. Despite relying heavily on the reliability of complex digital components and systems, many organizations fail to understand the level of cyber integration and dependency modern-day society requires. With such explicit dependency on these cyber mediums comes a responsibility to be aware of the many ways people and organizations are vulnerable. As such, research into the job roles and competencies of individual employees provides numerous insights to include the lack of proper cyber practices businesses and organizations fail to employ, as well as what skills are missing to properly implement good cyber practices.

Throughout the summer of 2021, open-source research was performed on various Idaho municipalities' websites, and in-person industry visits were conducted with businesses from several municipalities' branches. Specifically, the NIST (National Institute of Standards and Technology) 800-181 and National Initiative for Cybersecurity Education (NICE) Workforce Framework have been used to create Cybersecurity Competency Health and Maturity Progression model (CYBER-CHAMP). The NIST/NICE framework is a compilation of complex documents outlining cybersecurity fundamentals, viewed as the industry standard when it comes to cybersecurity foundations. As such, CYBER-CHAMP is designed to help organizations evaluate individual employees' roles and tasks within their job positions. This information was then used to access all employee tasks, which provided a detailed breakdown of what competencies are needed for a respective position. This helps to create a plan for how to train an employee for proficiency and cyber competency. This also allows for maximum return on investment (ROI) for the employee's organization.

Cyber Ignorance – The Root of the Problem

- This summer's research has shown top managers and leaders in many businesses and municipalities do not see the need for dedicated cyber personnel. In fact, many don't see the need for cybersecurity at all, neglecting the need to educate personnel with any kind of cyber responsibilities, knowledge, or training. However, this also appears to show that as organizations become larger, they increasingly begin to understand the importance of these positions and the associated risks of not having cyber-hardened networks. Unfortunately, and despite this realization, many still do not have an adequate grasp of their cybersecurity requirements or the amount of risk they carry. Though many organizations try to harden their networks, they often leave the human factor—the weakest link—uneducated and vulnerable.

The following three sections illustrate the two general cybersecurity stances organizations typically adopt (i.e., that cyber is important or cyber is not) based on the aggregate results of industry visits conducted during 2021; as well as open-source research conducted (City of Boise;

City of Boise Careers a-f; City of Meridian; Eide Bailly, 2020).

In an organization that believes cybersecurity is important, there are often one or two dedicated cyber positions. These employees are usually tasked with producing network layouts and firewall protocols. In addition, these cyber technicians tend to have a small amount of oversight from management personnel. They are subject to the dictates of managers who decide what cyber actions will and will not be taken, regardless of a general lack of cyber-knowledge. In some organizations there are Information Technology (IT) teams tasked with implementing physical changes deemed necessary by these cyber specialists. These positions are also tasked with day-to-day maintenance of the network and the handling of all support services— both internally and with any end-users. Employees in these positions often have a significant workload, and not enough time to complete it. As with any such overburdening, priorities are established that leave some tasks unfulfilled. When employees request additional help from management for additional cyber-literate employees, these requests are often ignored, leaving many of these tasks unattended.

A handful of Human Resource (HR) positions or training positions are tasked with the training of all employees—both new and old—on all the associated job requirements. Generally, only a small amount of cyber-training is included, but it is often glossed over and not explained properly by a qualified instructor. This is a problem because the HR trainer is generally not required to understand the assigned content. Some organizations have cyber training conducted by dedicated cyber professionals, but this has shown to be very uncommon.

Cybersecurity is not prioritized at all within some organizations. In such groups, teams consist of a small to medium sized team of IT personnel. These employees are tasked with designing network layouts, performing physical and virtual maintenance, and overseeing all support—both internal and external. These positions tend to have a far too much work to complete and not enough time to do it. In this scenario, it has been found these positions focus only on the most important tasks, which are assigned importance by management personnel who have little to no cyber knowledge. As a result, these IT teams often ignore the rest of their tasks, sometimes for days or weeks. This can be especially frustrating for the employee who is juggling all the responsibilities of keeping a business afloat. These IT professionals understand they need additional help to balance their workload. However, upper management typically holds all the cards when it comes to hiring and resource allocation. Considering cybersecurity is a preventative measure against compromise, management often sees cyber defense as unnecessary, or a bottomless pit of no-return investment.

A handful of HR positions or training positions are tasked with the training of all employees, both new and old, on all the associated job requirements. In this scenario, it has been found almost no cyber-training is given to any employees. These employees remain unaware of vulnerability risks, ensuring poor cyber-hygiene. The extent of the employees' cybersecurity awareness can be something like, "Don't go to shady websites while at work".

ICRP

Another problem found in organizations such as these pertains to legacy hardware and software. This is especially true in the industrial setting. Assembly/production-based businesses find it incredibly difficult to update their legacy equipment. According to comments made by organization representatives during industry visits, some of the most commonly voiced reasons as to why cyber improvements could not be made are:

- "It is too expensive."
- "We can't afford to have our production lines down for as long as it would take to upgrade them."
- "It isn't broken, so why fix it?"
- "The risk isn't high enough for us to update it."
- "We don't know how to do it."

Disconnection in the Cybersecurity Industry

There is a growing need for cyber personnel in the workforce, as evidenced by recent cyberattacks on critical infrastructure such as the Colonial Pipeline. Businesses, organizations, and entities around the globe are beginning to acknowledge the need for a trained cybersecurity workforce. However, the candidate pool for this cyber-ready workforce is very shallow. All the employers who are aware of this need are actively seeking highly skilled personnel to join their team. However, those entering the cybersecurity field often cannot meet the expectations for the roles and responsibilities they are expected to fulfill. Organizations need more than what is currently available, in terms of cyber skilled employees. Degrees held do not accurately describe knowledge, skills, and abilities held by an individual seeking cyber employment, and organizations typically do not have an effective way to filter through candidates to find those most suited for this specialized employment.

The research conducted for this paper research has also found departments within an organization often work separately. Many businesses and organizations have very little—if any—inter-department communication, especially when it comes to cyber hygiene. This is something organizations certainly need to address moving forward if they hope to become more cyber-hardened. This research discovery lies outside of the scope of this paper, but presents an interesting topic to be pursued, perhaps in future research.

Industry research has shown both local and state governments, as well as most businesses, have at least one dedicated cyber position. These positions focus primarily on the fortification of network infrastructure, keeping systems up to date, and the overall security of the network. Research found that even when these cyber positions were deemed critical by these organizations, there seemed to be a lack of requirements for cyber-team roles.

ICRP

The lack of trained professionals at these locations is a big problem. Not all the job roles of these positions were being met. This has led to a lack in performance because these individuals simply cannot accomplish all their position is responsible for. Those in charge of cyber-related matters are tasked with the creation and enrollment of cyber training to strengthen their organization.

In order to properly fulfill their duties, these cyber professionals must both perform assigned tasks and detail the specifics of those tasks to be learned by other employees. Our research shows organizations too often fail to ensure these duties are passed on correctly. Through continued research, it was determined complex cyber issues would be delegated to higher-level staff, though there are often no such personnel on staff. As a result, inexperienced workers are tasked with complex cyber roles beyond their skill level. Based on these findings, it is apparent there is a certain lack of importance placed on these jobs, resulting in a shortfall of cyber resilience. During industry visits, it became apparent there were many IT positions available, though these positions required little previous understanding of cybersecurity matters and implementation. To understand the lack of requirements in these roles, it is important to recognize how the positions function and how tasks are assigned.

Based on research, it was found some organizations have a range of positions consisting of programmers, system analysts, technicians, specialists, and administrators who all report to the chief officers and directors. Each of these positions are defined by specific tasks that help the organization to function. The programmer, for instance, would oversee software security compliance and create protocols to allow software to accept vendor updates. The system technicians or specialists would oversee support to the whole department, tasked with keeping the organization’s system running.

The IT team hierarchy identifies the different job positions well. At the head, a Services Director is responsible for the overall program. While some training is required for the Services Director, there is no specific cybersecurity related prerequisites. Next on the list is the Chief IT Officer and Supervisor (CIO), who is tasked with managing specific programs and other offices. While some cybersecurity knowledge is required, the CIO operates primarily in a managerial role and is not operating equipment. There are several specialists overseen by the CIO, including administrators and technicians responsible for the operation, security, and support of the machines. Although technicians in these positions operate the equipment, there are little to no cybersecurity-related prerequisites or knowledge required (City of Boise Careers a-f).

Although this is an example of a comprehensive IT team, there appears to be little cybersecurity training or background required. This could lead to an organizational culture where it is the task of others to engage with cybersecurity efforts. However, when this organizational structure is looked at more closely, it becomes clear these cyber responsibilities are barely covered at all. This leaves many business and municipalities in a state of cyber-unpreparedness.

ICRP

Cybersecurity Standards

The cybersecurity community has begun to understand what roles and tasks are needed for an organization to strengthen cyber resilience. However, there isn't any universally accepted standard for healthy cyber hygiene. The largest contributor to this problem is the varying definitions of what a cybersecurity standard is and how best to implement such standards. From the NIST article "Cybersecurity Standard" dated 2009:

"The International Organization for Standardization (ISO) defines a standard as 'a document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context,'" (Scarfone, 2009, p. 1).

Under this definition, a "standard" includes all elements of known cybersecurity techniques and practices. Specifically, these techniques have been reviewed and approved by multiple field professionals and consultants.

Guidelines and laws can easily be mistaken for cybersecurity standards. Misunderstanding the difference between these strategies can cause implementation errors and impair results. According to the NIST article, a guideline focuses on providing an organization with a general overview of how to improve cybersecurity (Scarfone, 2009, p. 3). By definition, a guideline does not hold the same credibility as a standard (Scarfone, 2009, p. 3). Although a standard is more accepted than a guideline, a standard is not held to the same legal standing as a law. In general, there are very few federal laws relating specifically to cybersecurity protocol. Most laws are directed towards federal and state government procedure as opposed to private company policies (National Conference of State Legislature, 2021). If a company fails to uphold a cybersecurity standard, they are at higher risk for cyberattack. The act of ignoring company standards does not have the same legal threat as law. The distinction between guidelines, laws, and standards can dramatically affect how cybersecurity procedure is enforced and upheld. Understanding the limits and usefulness of having a standard is the first step an organization can take to building a strong cybersecurity team.

Again, because there is no universally accepted standard for cybersecurity education and training, many organizations don't know which standards to employ when they begin to train employees. The ISO and International Electrotechnical Commission (IEC) has created international cybersecurity standards directed toward critical infrastructure safety. These standards include ISO/IEC 27001, 27002, 27031, and 27031 (IT Governance, n.d). The NIST 800-181 document is one of the more popular cyber standards used in the United States. This standard consists of five main areas of focus: identify, protect, detect, respond, and recover (NIST, 2014). Each word represents a different stage in the "cybersecurity lifecycle," and provides a different set of standards for each stage. Although these standards are recommended, they have yet to become common practice for many public and private organizations. Once a standard is decided upon, companies, organizations, and municipalities can begin training their employees to improve cybersecurity health.

ICRP

Cybersecurity Training

According to the U.S. Bureau of Labor Statistics, the need for cybersecurity professionals is predicted to increase by 31% over the next several years. It is reported in 2021 there will be 3.5 million unfilled jobs globally. Of the applicants applying for the cybersecurity positions fewer than one in four are qualified (U.S. Bureau of Labor Statistics, 2021). That said, there needs to be a better understanding how IT and OT professionals can become more competent in this field.

Cybersecurity is quickly becoming one of the most important areas for an organization to focus on as the number of hackers and the sophistication of their attacks are increasing. On May 12, 2021, an Executive Order signed by President Biden outlines the eminent need to improve the Nation's Cybersecurity (Exec. Order, 2021). This Executive Order emphasizes the importance of the Federal government and the private sector to partner together to protect our nation from malicious attacks. Current administration policy states that prevention, detection, assessment, and remediation of cyber incidents is a top priority and is essential to national and economic security.

Robert Herjavec, founder and CEO at Herjavec Group, said, "Unfortunately the pipeline of security talent isn't where it needs to be to help curb the cybercrime epidemic. Until we can rectify the quality of education and training that our new cyber experts receive, we will continue to be outpaced by the Black Hats." (Morgan, 2020).

What does one need to do to be considered cyber competent? Education alone does not satisfy this competency. Cybersecurity specialists must have working knowledge of existing training, industry certifications, clearances, and of course possess experience in the field. Some examples of the trainings and certifications in this field would include Security +, Network +, Certified in Risk and Information Systems Control (CRISC), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), and Certified Ethical Hacker (CEH), just to mention a few.

One problem facing would-be cyber defense professionals is the far-reaching and specialized training for different applications and network types. There are so many training courses available, it often delays organizations from launching cybersecurity programs. Considering a training program can be expensive and time consuming, organizations can find it difficult to decide on an appropriate training path. Training for duties not applicable to the tasks and responsibilities needed within a job role is wasted training. Basic cyber training is needed in all fields in the modern workplace, but a lack of focused training for those directly engaged in cyber defense can be a recipe for disaster.

One of the tools offering a solution to this problem is CYBER-CHAMP (Cyber-Competency Health And Maturity Progression). This innovative analysis tool tackles the problem of role-appropriate training head-on with its task analysis survey. Trainings cannot just be assigned by job position, as many people in IT and cyber with the same job title are assigned very different tasks. An employee in one company with the same job title as an employee from a different

company rarely does the same things. This is a problem CYBER-CHAMP helps solve. The tool has a catalog of over 1,000 trainings mapped to the specific roles in a given position, meaning the training an employee takes is directly applicable to an organization's day-to-day operations.

With most certifications, certain levels of experience and time in the field are required. For example, the CISSP requires 5 years work experience in the cyber field to even start the certification process ((ICS)², 2021). This makes this task of acquiring these types of advanced certificates more difficult for someone fresh out of a university who has not been working in the field.

As mentioned previously there is a substantial catalog of trainings available through CYBER-CHAMP that can be easily applied to most positions and roles. With hundreds of courses mapped to roles, it is easier for a cyber professional to understand training options and help build a successful career. Individuals fresh out of a university setting can also use the task analysis survey to view trainings available, as well as what each course would cost in time and money.

Another factor affecting management's decision to send an employee to training would be cost. The cost of training can be broken down to two factors: 1) the upfront cost involved with registering for training, and 2) the time required to take the training, limiting the employee's ability to do their regular job. Many trainings will require travel expenses as well as upfront fees, which can combine to put a significant dent in an organizational budget. All these factors can be a large deterrent as many think the money put into the cyber area does not return any financial benefit. This is . This is because cyber defense is a preventative measure, and such measures provide insurance against a worst-case scenario (such as a ransomware attack) and their benefits are often difficult to quantify. That is to say, preventing a successful cyberattack in the age of ransomware is more investment than expense.

As a result of additional training based on an employee's roles, the success rate against these attacks should improve significantly. Keeping IT and OT staff trained in cybersecurity will improve their ability to fight against these threats. Due to the ever evolving strategies of hackers, it is imperative all employees go through training every 4 to 6 weeks (Bambulas, 2020).

Findings/Results

Research performed during this internship has provided many insights into the way organizations think about cybersecurity, as well as how employees are trained on cyber practices. Furthermore, these insights can be summarized in one statement: Cybersecurity practices and guidance lacks uniformity and standardization. As such, an innovative tool is needed to help organizations target their training efforts and offer actionable solutions in a dynamic cyber defense environment. One such tool is the CYBER-CHAMP model developed at the Idaho National Laboratory. This model can be used to promote an organization's cyber hygiene and help train individual employees to be more cyber competent. The proliferation of this tool and its effectiveness can solve the numerous cyber vulnerabilities currently widespread in many industries and businesses.

ICRP

Discussion and Concluding Thoughts

It appears possible for an organization to build a cyber-ready workforce if the organization has the time and financial resources to train and educate employees based on roles and tasks. Very few tools exist to help an organization do this. However, CYBER-CHAMP is in the process of becoming one of these tools. Concerning the interns' experience and feedback received from utilizing CYBER-CHAMP during industry and municipality visits, it would be beneficial to develop this tool into a more user-friendly form. To this end, there is a CYBER-CHAMP web version currently under development.

Several users were also confused by some of the technical portions of the model that did not directly involve their fields of work. As such, refining the model down into specific modules or core 'customer bases' would make presenting the specifics of the model easier and less intimidating for less technical users. Additionally, further mapping of responsibilities to roles (such as which roles carry a legal burden of cyber risk) will also help flesh out the model into new avenues and make it more robust and applicable to the widest possible audience.

ICRP

References

Bambulas, N. (n.d.). *How often should you do cybersecurity awareness training? business technology.* Managed. https://www.gflesch.com/elevity-it-blog/how-often-should-you-do-cybersecurity-awareness-training#:~:text=The%20sweet%20spot%20for%20security,is%20every%204%2D6%20months

Biden, J. (2021, May 12). *Executive order on improving the nation's cybersecurity*. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

City of Boise. (2021). *City of Boise Employee Policy Handbook* (pp 332-333).

City of Meridian. (n.d.). https://meridiancity.org/.

Chief Information Officer. Job Descriptions | City of Boise Careers. (n.d.-a). https://www.governmentjobs.com/careers/boiseid/classspecs/1381964.

Cybersecurity and Infrastructure Security Agency CISA. (n.d.). Cybersecurity education & Career development. https://www.cisa.gov/cybersecurity-education-career-development.

Cybersecurity and IT Security Certifications and Training: (ISC)². Cybersecurity and IT Security Certifications and Training | (ISC)². (n.d.). https://www.isc2.org/.

Data Engineer. Job Descriptions | City of Boise Careers. (n.d.-b). https://www.governmentjobs.com/careers/boiseid/classspecs/1382061.

Data Services Senior Manager. Job Descriptions | City of Boise Careers. (n.d.-c). https://www.governmentjobs.com/careers/boiseid/classspecs/1379059.

Eide Bailly. (2020). *City of Meridian, Idaho: FY 2020 Audit* (pp 6, 44).

Field Tech Lead. Job Descriptions | City of Boise Careers. (n.d.-d). https://www.governmentjobs.com/careers/boiseid/classspecs/1382032.

Hatzes, L. (2020, Nov. 16). *History*. National Institute of Standards and Technology (NIST). www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/history

IT Cybersecurity Analyst II. Job Descriptions | City of Boise Careers. (n.d.-e). https://www.governmentjobs.com/careers/boiseid/classspecs/1381870.

IT Cybersecurity Lead. Job Descriptions | City of Boise Careers. (n.d.-f). https://www.governmentjobs.com/careers/boiseid/classspecs/1381960.

ICRP

IT Governance. (n.d.) Cybersecurity standards list. https://www.itgovernanceusa.com/cybersecurity-standards.

IT Physical Security Engineer Sr. Job Descriptions | City of Boise Careers. (n.d.-h). https://www.governmentjobs.com/careers/boiseid/classspecs/1381896.

IT Programmer Analyst Sr, ERP. Job Descriptions | City of Boise Careers. (n.d.-i). https://www.governmentjobs.com/careers/boiseid/classspecs/1382064.

IT Systems Analyst. Job Descriptions | City of Boise Careers. (n.d.-j). https://www.governmentjobs.com/careers/boiseid/classspecs/1382074.

Morgan, S. (2020, Aug. 4). *Cybersecurity talent crunch to create 3.5 million unfilled jobs globally by 2021*. Cybercrime Magazine. https://cybersecurityventures.com/jobs/.

National Institute of Standards and Technology (NIST). (2014). NIST Cybersecurity Framework. https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics#framework

National Conference of State Legislature (NCSL). (2021, Apr. 1). Cybersecurity legislation 2020. https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2020.aspx

Petersen, R., Santos, D., Wetzel, K., Smith, M., & Witte, G. (2020, November 16). *Workforce Framework for Cybersecurity (NICE Framework)*. Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final

Scarfone, K., Benigni, D., & Grance, T. (2009). *Cybersecurity standards*. National Institute of Standards and Technology (NIST). https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152153

Training and Organizational Development Coordinator. Job Descriptions | City of Boise Careers. (n.d.-k). https://www.governmentjobs.com/careers/boiseid/classspecs/1382010.

Training and Development Systems Administrator. Job Descriptions | City of Boise Careers. (n.d.-l). https://www.governmentjobs.com/careers/boiseid/classspecs/1381969.

U.S. Bureau of Labor Statistics. (2021, April 9). *Information security analysts: Occupational outlook handbook*. U.S. Bureau of Labor Statistics. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

ICRP

Appendix A

COSTAR

COSTAR is a model-method created by the INL. It is used to add value to presentations, by giving structure to one's ideas and ensuring key details and talking points are not left out. Below is the key points and introduction points taken out of a presentation given on CYBER-CHAMP by this summer's interns.

- Introduction:
  - Last year cyber-attacks cost the world just under $1 Trillion.
  - One in three people will be a victim to cyber-attacks.
  - Using NIST/NICE framework CYBER-CHAMP, INL employees and interns worked with various organizations (municipalities, businesses, and institutions) throughout Idaho to better understand how they view/value cybersecurity by assessing their policies, job roles and overall cyber hygiene.
- Customer:
  - Currently, local governments and businesses
  - Applicable to all businesses
- Opportunity:
  - Focus on training employees, improving cybersecurity, and maximizing ROI spent on behalf of an organization's cybersecurity improvement.
  - ROI
- Solution:
  - Cyber-CHAMP is a model that allows for accessing the competencies of individual employees and develops a 'pipeline' to train them to proper cyber-hygiene.
- Team:
  - SS Cyberian and the Organization's management team.
  - Abigail Moody, Andrew Killpack, Autumn Clark, Jason Forbush, Kyler Combe, Thomas Upchurch, Shane Stailey
- Advantage:
  - There is no standardization for cybersecurity. The interns are actively seeking potential solutions for this.
  - There currently is no software or program directing employees to trainings specifically based on what roles and tasks they are must accomplish on a given day.

ICRP

  - Giving a clear idea on how to be compliant with the bodies that do exist by having all standards in a format easier to understand and implement.

- Result:
  - Individual cyber competency for the workforce.
  - Companies will achieve greater ROI.
  - Employees with know how to better complete their job on an individual level.
- Feedback Received Key Points:
  - Did a good job with the introduction and explaining how the model works at a low level.
  - Perhaps add how we do this. How do we train job posters on the best way to create new job postings, addressing the needed requirements?
  - Had someone asking for information and wanted to have a further conversation.
  - Liked how it aims to standardized cybersecurity - Stronger if quantified some steps for standardization.
  - Liked how the presentation began with framing the problem in terms of financial impact.
  - More willing to fund it if there was more talk about robustness of the model. That is, if the cyber landscape changes, how will the model change with it?

ICRP

Appendix B

Cyber-CHAMP Lite

Interns Andrew Killpack and Jason Forbush were tasked with creating a model of Cyber-CHAMP that could be provided to a potential customer to give a basic understanding of how Cyber-CHAMP works. The goal of this is to provide a foundation to build upon when presenting the actual Cyber-CHAMP model.

Cyber-CHAMP Website Development

About halfway through the summer, intern Autumn Clark was recruited to work on the development of a website version of the Cyber-CHAMP task analysis survey. More specifically, he worked on development of the framework for the Individual Dashboard an individual will see after they log into their account. Currently, the web version has the basic framework of the HTML version, but still needs substantial work to get the log-in and dashboard screens working and sufficiently polished.

Cyber Risk Mapping

Around the same time, intern Abigail Moody was asked to work with INL mentor Jade Hott to design management roles within an organization. Then, using Dr. Cresson Wood's collection of cyber responsibility, they will be mapping cyber-related legal responsibility to the preassigned management roles. Currently, all the roles have been defined and a spreadsheet has been developed to begin mapping.

Mapping Governing Bodies Policies

As well, intern Kyler Combe was asked to map the policies of the governing body known as ISA62443, to make it more applicable to the Cyber-CHAMP model. This was also an effort to make the polices more manageable and easier to understand; and apply to an organization that would need to comply with their regulations.

ICRP

Appendix C

Interns' University Enrollment

Brigham Young University – Idaho: Andrew Killpack

College of Southern Idaho: Thomas Upchurch

Idaho State University: Autumn Clark, Jason Forbush, Kyler Combe

University of Idaho: Abigail Moody