Understanding How Organizations Handle Cybersecurity

August 2021

Team Quiver

Andrew Cornelius, Brigham Young University-Idaho
Austin Crouch, College of Western Idaho
Felino Macatuno, University of Idaho

Mark Jackson, Idaho State University
William Johnson, University of Idaho

INL Mentor

Donaven Haderlie

Abstract

If there is anything we can learn from the media, it is the frequency and severity of cyber-attacks is increasing and there are not enough qualified people to combat the risk organizations are facing. Current estimates say there are 3.5 million available cybersecurity related jobs globally and there has been a 350% growth in cybersecurity jobs since 2013 (Group, 2020). The Idaho Cyber Research Project (ICRP) is focused on finding an implementing solution to the problems in the workforce development pipeline. Our team consists of Cohort 2 of the ICRP, we are tasked with solving issues faced by organizations hiring new cyber personnel. To provide solutions to these issues we focused our research on four components of workforce availability and competency: resume and transcript analysis, apprenticeships, cyber incident response plan development, and adversarial mindset training. From this research we have produced the following focus areas and subsequent steps for each component of workforce capability: transcript and knowledge skills abilities (KSA) focused analysis, cybersecurity apprenticeships programs, the value of an adversarial mindset, and a guide to setting up cyber incident response plans for underprepared organizations. These solutions can be further developed and implemented to reduce the gap in workforce demand and talent.

Table of Contents

Introduction

Ransomware attacks continue to increase, where an “organization became a victim of ransomware every 10 seconds in 2020” [1]. Most notably, cyberattacks in the healthcare industry "jumped 37% in 2020 as cyber-criminals sought to capitalize on organizations distracted by the fight against COVID-19" [1]. Therefore, it is imperative to advance cybersecurity practices used by members overseeing United States critical infrastructures to preserve the rebounding economy and daily societal functions. According to the National Security Agency (NSA), "Cyber threats to U.S. national and economic security increase each year in frequency, scope and severity of impact. Cyber criminals, hackers, and foreign adversaries are becoming more sophisticated and capable every day in their ability to use the Internet for nefarious purposes," using techniques such as "remote hacking intrusions, the placement of malware, spear phishing and other means of gaining access to networks and information" (NSA, n.d.). As shown this past year, the dependency on wireless technology must be balanced with the integrity of Internet networks to mitigate these cyberattacks.

The pandemic has negatively impacted the retention rates of cybersecurity professionals, which dropped by four percent. It has also opened more system vulnerabilities for adversaries to exploit, as some company networks have prioritized availability over confidentiality (Security, 2021). Entities operating critical infrastructures are generally unprepared to tackle cyber-related issues, as "61 percent of cyber security teams are understaffed" and "55 percent (of companies) say they have unfilled cyber security positions" (Security, 2021). According to the NSA, "Denial of service attacks disrupt business and undermine confidence," costing industries billions of dollars each year; therefore, entities in the public and private sector must act as a cohort in addressing these issues (NSA, n.d.). As researched by Cybersecurity Ventures, "There will be 3.5 million unfilled cyber security jobs in 2021" (Kroll, 2019). Despite requiring a cyber-related bachelor's degree for most entry-level positions, only 27 percent of companies indicated recent graduates are well-prepared (Security, 2021), "50 percent (of companies) say their cyber security applicants are not well qualified," and "31 percent say HR regularly understands their cyber security hiring needs" (Security, 2021).

ICRP aims to provide solutions to progress the cybersecurity workforce development pipeline. With issues such as finding qualified candidates and retaining cyber-talent, it is paramount to recognize inconsistencies in current cyber-management practices. The Cohort 2goal is to understand how organizations can better understand their cybersecurity needs.

An Analysis on Resume and Transcript Filters

Background

Due to the popularity of online recruiting websites like Indeed.com, the geographic range for recruiting candidates has greatly expanded, as Indeed.com alone hosts 250 million users each month and 10 new job postings per second globally (Indeed, 2020). Moreover, this convenient job search process can be a bottleneck for Human Resources (HR) departments who are tasked to parse through resumes and transcripts. As a result, most HR departments have turned to

Applicant Tracking Systems (ATS) to “assist with recruitment and hiring processes” and “attract applicants and to predict a candidate’s fit for a position” (Shields, 2017; Heilweil, 2019). ATSs enables businesses to “efficiently collect information, organize prospects based on experience and skill set, and filter applicants” (Hudson, 2021). Specifically, “ATSs parses a resume’s content into categories and then scans it for specific keywords to determine if the job application should be passed along to the recruiter” (Augustine, n.d.). In fact, the Idaho National Laboratory (INL) uses Taleo, an ATS, to aid in the hiring process; however, INL’s hiring practices remains a manual process, not relying heavily on an ATS.

Issues with an Applicant Tracking System

The role of an ATS is to “essentially weed out unqualified applicants so the recruiter can devote his or her time to evaluating the candidates who are more likely to be a match for the position” (Augustine, n.d.). Therefore, an ATS is only “apt to toss the *least-qualified* candidates, rather than identify the applicants who are the best fit” (Augustine, n.d.). ATSs only looks for resumes that meet the exact requirements of a job posting; for instance, “recent college graduate, borderline candidates or those switching careers will be at a disadvantage” (Mukherje et al., 2014). Furthermore, ATSs are often “unreliable and can reject resumes for unnecessary reasons, such as if the scanner is unable to read [the resume] properly” (Mukherje et al., 2014). Moreover, there is a “strong possibility that certain keywords in a vast majority of job applicant’s resumes are exaggerated. Some candidates purposely stuff his/her resume with keywords so that their resume is selected by the system.” (Mukherje et al., 2014). This malpractice is inefficient for both parties. Finally, some grade point average (GPA) filters may mask a candidate if it falls below a threshold, removing a possible great candidate.

Next Steps

With inconsistencies in ATSs, how can INL’s ICRP help organizations better analyze resumes and transcripts beyond GPA when recruiting cyber-talent? Typical job applications require candidates to submit an academic transcript; however, in interviewing Idaho organizations, transcripts are underutilized and primarily used as proof for academic progress, not academic interest. Terms like Computer Science, Cybersecurity, or Computer Engineering used to describe cyber-positions are too broad and branches to different subfields, which may result in an overgeneralized job posting causing inefficiency for HR. The requirement of academic transcripts should move beyond GPA; therefore, to create a great, long-lasting impact for INL design and implement an ATS tailored for the cyber-industry by preserving current ATS practices and combining features from CyberKnights.

CyberKnights maps college courses specified by universities to a Knowledge Area (KA) from the necessary university adopted NICE-NIST framework. With CyberKnights, a recruiter can see which KAs an individual has achieved in their coursework. A dashboard or website platform can show recruiters if a candidate’s KAs are best for a certain role. Using a candidate’s transcript, this method can match a person’s academic interests in the courses they have already taken to KA’s needed in industry, minimizing the notion that “classwork” does not apply directly to the workforce. KA's gained by completing apprenticeships or extra-course work can also be applied.

Apprenticeships

Background

With the increase in recent cyber-attacks organizations are needing more individuals that have professional experience with cybersecurity. This need for more cybersecurity personnel has created a void of 314,000 unfilled cybersecurity positions across the United States at the beginning of 2021 (Inglet, 2020). Worldwide there is a shortage of 3.5 million unfilled cybersecurity positions (Perhach, 2018). The causes of these gaps in cybersecurity are that in the past decade many organizations have switched to a more information technology (IT) focused design and are increasingly relying on cloud base and remote services to improve their organization's performance and flexibility. Organizations have also automated many of their supply chains, moving away from the older manual supply chains. All these technological improvements to organizations, across sectors, has created a vast need for more IT individuals to help manage and troubleshoot the newly implemented technology. This has made it more difficult for organizations to secure their systems and, by being more connected, have opened themselves up to more cybersecurity risks.

Solution

To combat this increased cybersecurity risk organizations are looking to hire more cybersecurity professionals to secure their systems. The problem is there is a skills gap between the candidates that apply to these positions and the professionals that have been in the industry for years. These graduates cannot easily receive the experience they need to be considered for many of the entry-level positions within the cybersecurity field. Thus, creating a skills gap within cybersecurity careers. For entry-level positions many organizations are looking for individuals that already have cybersecurity experience instead of individuals who have none.

One solution to this issue is to give individuals with no career experience the chance to gain hands-on experience through apprenticeships. Apprenticeships give individuals the chance to learn from professionals who have the experience organizations look for on a resume. Apprenticeships benefit organizations by giving them the opportunity to grow their current workforce while training more individuals that produce quality work. Organizations can reduce the turnover costs of training new employees by having these apprentices who are loyal and engaged in their operations. Apprenticeships also commit individuals by contract to work for an organization for a certain amount of time after their apprenticeship is completed, thus increasing retention rates, especially within the cybersecurity field.

Cybersecurity apprenticeships are a recent addition to the scene. These apprenticeships are an important part of how we can start to close the skills gap the cybersecurity field faces. With cybersecurity apprenticeships individuals can receive hands-on experience from cybersecurity professionals. These mentors can give apprentices a better understanding of the world of cybersecurity, as well as knowledge of current trends within the field.

Next Steps

In a meeting with INL's HR department it was found they are trying to get their own cybersecurity apprenticeship program set up so they can work out the issues within the curriculum. We believe it would be best to be involved in this process of creating the apprenticeship curriculum for this apprenticeship. Visiting more organizations to specifically assess what they believe should go into an apprenticeship program will be useful in creating a general apprenticeship program for cybersecurity. This will give future projects the opportunity to encourage organizations to use apprenticeship programs and show them the value apprenticeships can bring to an organization.

A Hacker's Mindset

Background

What is it that makes a successful hacker? At first glance of this question, you might begin to write a laundry list of technical skills attributed to the tasks a hacker or pentester might need to complete, however we believe the question is much deeper than that.

It's important to understand the terms 'penetration testing' and 'ethical hacking' often connotate network and software vulnerability testing, but the idea is much broader. Avoiding this connotation is critical when gaining the support of management and key stakeholders in an organization due to how common it is to outsource such tasks, as well as when recruiting or attracting talent. Using terms like 'red teaming' or 'adversarial mindset' may be more appropriate when describing what an organization needs from a cybersecurity professional, in addition to or separate from the defensive roles the organization is looking to fill, particularly when speaking internally, but also when crafting a job posting. In essence, you need to know how something might fail, but more importantly how someone might think to make it fail before you know how to protect or secure it. These skills are much more difficult to teach than the technical steps and processes behind specific tasks, and equally if not more difficult to advertise or recruit for.

There isn't a single turnkey solution for securing an organization's infrastructure, or else organizations would not need to fill dedicated cybersecurity positions. The specifics to mitigating digital risk vary from product or service and change drastically depending on implementation. This kind of variability outlines the requirement for cybersecurity professionals to think critically about their organization's infrastructure and resources and be capable of coming up with creative solutions to layered, complex problems. The field of cybersecurity is constantly evolving, staying up to date requires a certain level of attention and interest in these topics, which is something that can't really be taught. An organization needs to be aware of the need for continuous learning on the job, and not only create an environment that fosters this but also write job postings that effectively advertise this as not only a requirement, but a benefit of the position.

Rayome (2017) found a few common pitfalls in cybersecurity job postings.

1. Demanding too many skills: This is often in the form of requiring mastery of many highly specialized skills along with soft skills, like project management and communication.
2. Poor compensation: Often seen in the form of the organization looking for an individual to fill multiple roles under a salary that would only fit one of the roles.
3. Overlooking talent: Current employees, recent graduates, and women are all untapped resources.
4. Poor work/life balance: Cybersecurity tends to be a passion and hobby as well as a job. Employees are often responsible for responding to alerts whenever they might occur.
5. Inefficient recruiting process: Lengthy and cumbersome recruiting processes can cause the organization to lose candidates.

Solutions

Rayome (2017) proposed a few potential solutions to the issues identified above.

1. Prioritize which specialized skills are most important for the organization to have in-house and fill the gaps using service providers.
2. Companies need to be selective about the skills they truly need on staff and offer competitive rates for those skills.
3. Job rotation programs where people try out security roles for a set amount of time can help identify talent existing already within the organizational structure. Partnering with universities to create internships and jobs for recent graduates can help build the talent pool.
4. Offering flexible hours and remote working arrangements can help make up for the level of commitment the positions may require.
5. Companies need to network the same way employees do, offering referral bonuses can help bring in talent.

In line with problem 3, apprenticeship programs can be a great way to bring in talent early in apprentices' careers and allow the employee and company to grow together. The Idaho Department of Labor offers a great deal of assistance to organizations looking to engage in a registered apprenticeship program.

The HR department needs to work closely with IT and other departments when hiring a cybersecurity professional. Creating tools and materials HR associates can use to aid them in hiring cybersecurity professionals could help close the cybersecurity workforce gap and make gaining and maintaining employment in this field more successful and rewarding. A handbook containing processes or directed communication templates for HR to leverage when posting an open position could be a valuable resource that helps bridge communicative barriers and make job postings clearer.

It is particularly important hiring managers understand what skills are necessary and how they might relate to character types or behavioral traits. In a meeting with INL's HR team they illustrated the Cybercore's working environment as very hands-off from management and personal to the employees, recognizing they do their best work unburdened by the social stressors that can come with office life. Recognizing an employee's needs is important in any part of an organization, autonomy and minimizing certain distractions seems to be a running trend with highly successful cybersecurity professionals. Given this trend, if material or a handbook is to be created and given to hiring managers, there should be some inclusion of what to expect in terms of character type or accommodations to avoid turning away potentially stellar candidates due to communicative or social hurdles.

What about organizations that may need a cyber professional but don't know it yet? At this stage it's unclear whether motivation for those organizations to step up to the plate is going to come due to regulation, legislation, or a national call to shore up to an ethical responsibility. However, there is a clear opportunity for professionals in the field and organizations like INL to help industry get ahead of the game before it becomes a national issue. As true today as it was in 1799, a good offense is the best, if not only defense (Washington, 1799).

Next Steps

Materials should be developed for hiring managers to reference when collaborating with stakeholders and department managers requesting additional staff. This could be with varying levels of detail, starting with a PowerPoint-style high-level overview, then a handbook, perhaps leading to a full publication. This should be a training opportunity for HR associates to effectively hire Cyber professionals, and these materials should be concise and detailed in a variety of approaches.

Industry leaders should be encouraged to help other organizations recognize the importance of achieving good cyber-hygiene by opening conversations and being transparent about cyber events they may have faced, or that they have chosen to prepare for. INL can facilitate this growth for ICS related industries while respecting operational and safety necessities.

Cyber Incident Response Plan

Background

Our cohort had the opportunity to meet with various organizations to learn about their hiring process and cybersecurity posture. The CIO of a local hospital verbalized how nice it would be to have a playbook or template to refer to during or before a cyber-related incident. Feedback from other organizations informed us not all companies or organizations have a cyber incident response plan. This led to researching the importance of a cyber incident response plan and how to help organizations create their own. Cybersecurity incident response has become an important component of IT and operational technology (OT) programs. "Cybersecurity-related attacks have become not only more numerous and diverse but also more damaging and disruptive"

(Technology, 2012). “An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services” (Technology, 2012).

Solutions

With so many resources and tools available to structure a cyber incident response plan, it can be difficult to know where to begin. Our goal is to create an easy-to-use playbook that guides any organization looking for help or advice regarding their cybersecurity posture. The playbook will be an easy-to-understand reference tool all employees will be able to use. The playbook will follow the incident response life cycle phases found in NIST SP 800-61r2. The focus and structure of the playbook will utilize the incident response life cycle phases: Preparation, Detection & Analysis, Containment Eradication & Recovery, and Post-Incident Activity. General information and guidance on these phases, and important steps when creating a response plan, will be the focus of the playbook. The playbook is not intended to be a complete guide to create an incident response plan but to provide sources and direction to find deeper understanding and knowledge on how to create one.

Next Steps

The next step for this focus area will be to continue creating an easy-to-use playbook. Many sources have been gathered and important information has been highlighted from them as starting points for the playbook. Critical information from the sources frameworks needs to be added to the playbook for quick reference and direction. The end goal will be a physical guide that can be handed to organizations needing help creating a response plan or guidance on where to find information and resources to help them.

Conclusion

With cyber-incidents at the spotlight of national and local security, the implementation of these steps aim to lubricate the cybersecurity workforce development pipeline. An ATS combined with a robust apprenticeship program enables individuals to align their academic and career goals to the needs of the industry. A collection of materials for organizational stakeholders to reference when filling cyber roles and developing incident response plans will strengthen an organization’s objectives for the long term and put them in a position to not only react quickly and appropriately to a cyber incident but prevent one from occurring in the first place.

References

Augustine, A. (n.d.). *What's an ATS-Friendly Resume? And How to Write One*. Retrieved from TopResume: https://www.topresume.com/career-advice/what-is-an-ats-resume

Borsellino, R. (n.d.). *Beat the Robots: How to Get Your Resume Past the System and Into Human Hands*. Retrieved from themuse: https://www.themuse.com/advice/beat-the-robots-how-to-get-your-resume-past-the-system-into-human-hands

Group, H. (2020). *Cybersecurity Ventures predicts there will be 350% growth in open cybersecurity positions from 2013-2021*. Retrieved from Herjavec Group: https://www.herjavecgroup.com/2019-cybersecurity-jobs-report-cybersecurity-ventures/

Heilweil, R. (2019, December 12). *Artificial intelligence will help determine if you get your next job*. Retrieved from Vox: https://www.vox.com/recode/2019/12/12/20993665/artificial-intelligence-ai-job-screen

Hudson, K. (2021, June 2). *What is an Applicant Tracking System?* Retrieved from Jobvite: https://www.jobvite.com/blog/recruiting-process/what-is-an-applicant-tracking-system/

Indeed. (2020). *About Indeed*. Retrieved from Indeed: https://www.indeed.com/about

Inglet, M. (2020, January 10). *'There's a massive void': Need for cybersecurity professionals on the rise in Idaho and the U.S.* Retrieved from 13NewsNow: https://www.13newsnow.com/article/tech/theres-a-massive-void-need-for-cyber-security-professionals-on-the-rise-in-idaho-and-the-us-shortage-internet-cyber-crime-hackers-online/277-c12f3b61-433d-42ef-b1b5-f1ee43cd488c

Kochling, A., & Wehner, M. C. (2020). Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development. *Business Research*, 795-848.

Kroll, S. T. (2019, March 6). *Only 3 Percent Of U.S. Bachelor's Degree Grads Have Cybersecurity Related Skills*. Retrieved from CYBERCRIME MAGAZINE:

https://cybersecurityventures.com/only-3-percent-of-u-s-bachelors-degree-grads-have-cybersecurity-related-skills/

Mukherjee, A. N., Bhattacharyya, S., & Bera, R. (2014). Role of Information Technology in Human Resource Management of SME: A Study on the use of Applicant Tracking System. *IBMRD's Journal of Management and Research*, 1-22.

NSA. (n.d.). *Understanding the Threat*. Retrieved from National Security Agency Central Security Service: https://www.nsa.gov/what-we-do/understanding-the-threat/

Perhach, P. (2018, November 7). *The Mad Dash to Find a Cybersecurity Force.* Retrieved from The New York Times: https://www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html

Rayome, A. D. (2017, March 29). *5 reasons your company can't hire a cybersecurity professional, and what you can do to fix it*. Retrieved from TechRepublic: https://www.techrepublic.com/article/5-reasons-your-company-cant-hire-a-cybersecurity-professional-and-what-you-can-do-to-fix-it/

Sayegh, E. (2020, September 22). *As The End Of 2020 Approaches, The Cybersecurity Talent Drought Gets Worse*. Retrieved from Forbes: https://www.forbes.com/sites/emilsayegh/2020/09/22/as-the-end-of-2020-approaches-the-cybersecurity-talent-drought-gets-worse/?sh=c40d1f05f868

Security, H. N. (2021, May 5). *61% of cybersecurity teams are understaffed*. Retrieved from HELPNETSECURITY: https://www.helpnetsecurity.com/2021/05/05/understaffed-cybersecurity-teams/

Shields, J. (2017, December 21). *What is an Applicant Tracking System?* Retrieved from Jobscan: https://www.jobscan.co/blog/what-is-an-applicant-tracking-system/

Technology, N. I. (2012, August). *Computer Security Incident Handling Guide.* Retrieved from NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Washington, G. (1799, June 25). *From George Washington to John Trumbull, 25 June 1799*. Retrieved from National Archives: https://founders.archives.gov/documents/Washington/06-04-02-0120

Appendix

Appendix A: Team Quiver's Influencers and Impacts

Industrial Cybersecurity Community of Practice (ICSCOP) Impacts

Interviews with representatives in the ICSCOP and organizations in Idaho indicates cybersecurity is a growing concern and finding qualified professionals remains the top priority. The following table is a list of Cohort 2's influencers and impacts that pointed the direction of Team Quiver's research topics:

INFLUENCERS	IMPACTS
Meeting with Department of Labor about apprenticeships	Communication with organizations about apprenticeships
Meeting with CyberKnights to discuss organizational side of their site	CyberKnights can be used to assess an organization's cyber hygiene
Collaboration with other cohort's project areas	Gained greater understand of how project areas coincide
Organizations are doing annual cybersecurity briefings	Does not give employees practice looking for things like phishing
Organizations not sure of their cybersecurity needs	Organizations are outsourcing their cybersecurity needs rather than having in-house cybersecurity
Organizations are outsourcing cybersecurity infrastructure	Organizations have less control and knowledge of their infrastructure, and become reliant on the partner

Appendix B: Notes

Meeting with INL HR

What kind of cyber roles does INL commonly fill? Anything that might be like a red team or penetration tester?

- Depends on how technical you are
- Ralph's team does a lot of the training for those areas
- Cybercore division is less on the training, less on the business facing side, more hardware or technical roles – cyber experts in the area of hardware – firmware etc – not great communicators
    - Very difficult to find these individuals
    - Hard to engage with

How do you locate the appropriate talent?

- Work closely with the manager before a job is posted at all
- Strict set of rules to follow for minimum credential or experience

Do you have tools that help filter or analyze resumes?

- Taleo is their applicant tracking system
- Taleo isn't screening for experience, screening a very manual process for us

Have you noticed individual traits or personalities that perform well in these roles, or make it feel like a 'no brainer' to hire them? How do you go about quantifying or testing an applicant to see if those traits are present?

- Asked a question – how does your home lab look like? What are your technical hobbies outside of work?
    - They always have some sort of technical hobby outside of work
    - Shows innate curiosity that seems naturally coupled with being a hacker that works with Cybercore
    - Always like building things out of nothing
- Putting hobbies and extracurriculars on a resume is good for this type of role
    - Showing analytics on a thing they did
- One person programmed a George Foreman grill to interface with his phone
- Whenever someone has something interesting on their resume it makes the process more exciting for the recruiter

Who comes to you with requests? how does a manager communicate a need to hire to HR?

- They need to make it simple for the HR person
    - The stuff they do is so far above and beyond an HR person in general, needs to be simplified
    - Give questions to ask, keywords to look for
    - Rule of thumb, if you talk a lot like you know what you're doing and are pleasant that will work well

Questions for Organizations

- What is your hiring process?
    - Keywords
    - Resumes
    - Transcripts

Evaluating Organization's Cybersecurity

    - Platforms
- What type of cybersecurity training do you have?
    - What practices do you employ to keep employees aware?
        - Phishing email practice
        - Meetings
- What are the current IT needs of an organization?
- Are KSATs more important than a degree to that field?
    - Some say yes
- Can CyberKnights be made to accommodate the OT side of cybersecurity?
- Are apprenticeships something that you are interested in?
    - Tell how it is relatively simple to set up an apprenticeship through the Department of Labor
- What does HR/IT define as OT?
- Does your organization currently utilize resume filters to recruit prospective cybersecurity employees? If so, what is that process like?
    - If you could create a perfect job posting, what would it include and why?

Cyber Apprenticeship Findings

- The Department of Labor has an apprenticeship program already set up for a Cybersecurity Support Technician that IT departments can use to retain new employees.
- https://www.apprenticeship.gov/apprenticeship-occupations/listings?occupationCode=15-1212.00
- They do not have apprenticeships for the ICS side of OT
    - Would it be hard to find jobs that do cybersecurity for ICS?
        - Would those jobs be able to have apprenticeships?
- Research how an organization can set up apprenticeships and the steps that need to be taken
    - Employers can use this site to express interest in an apprenticeship program that already exists or create their own.
    - They can use the site to find an apprenticeship they are interested in and they will then be contacted by an apprentice consultant and receive training plans from the Department of Labor.
- How can organizations be convinced the apprenticeships are equal to 4-year degree?
- Organizations must have a curriculum plan in place for apprenticeships and that may be the hardest thing for an organization.
- How INL apprenticeships are going for Cyber, both IT and OT?
- What type of curriculum had to be developed, or what type of curriculum did you use?
    - Apprenticeships for Journeyman and crafts through CBA decide what curriculum is used. Works with unions to develop those curriculums.
    - Getting apprenticeships for cyber approved and are in the works to get apprenticeships for cyber curriculum done.
- How did you get the apprenticeships out there and to applicants?
- Would you consider an apprenticeship experience the same or on a similar level as 4-year degrees?
    - Give credit for apprenticeships similar way as internship in ways of weighing a candidate.
    - Emails for HR meg.duba@inl.gov , shannon.obrien@inl.gov

- Apprenticeship 101 is for organizations that want to start apprenticeships.
- On the job experience is supplemented with related technical instruction.
- Apprentices agree to a training wage that increases as they go through the apprenticeship.
- DOL only works with registered apprenticeships.
- Industry Recognized Apprenticeship Programs (IRAPs) are national and compliment registered apprenticeships.
    - IRAPs are used when RAPs cannot approve an apprenticeship
- Colleges offer apprenticeships that partner with employers. The college then provides the education required to work with organizations.
- In-house Corporate Apprenticeships.
    - Does not follow state or national standards.
- ApprenticeshipIdaho
    - The IDOL will be under this new name.
- The IDOL acts as a liaison between employers and the USDOL.
- The IDOL writes standards, helps navigates the registration process, and helps consult on standards development.

CyberKnights Feedback

- Shows the KSATs what a specific role needs, but not ways to acquire those KSATs.
- Good repository of a lot of KSATs that are in cyber.
- After completing the hard and soft skills assessments there are not a lot of other things that an individual can do to improve themselves.

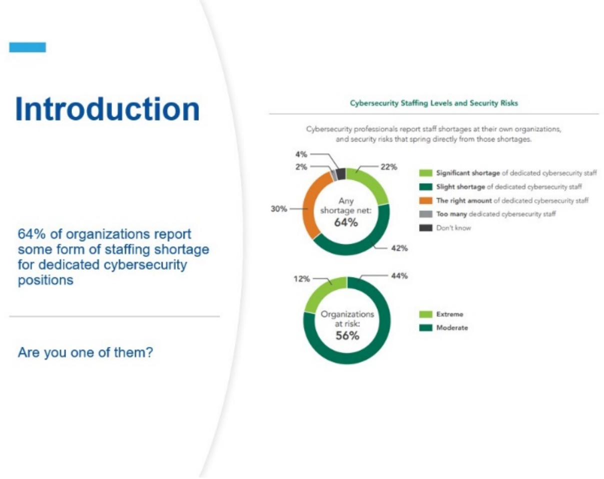
Sandbox

- How do the KSAs add up to the Total KSAs?
- The dashboard charts are useful and show some important information about the organization and the certifications that your employees have.
- Looks like the Educators section needs content on the courses that academia offers.
- Some sort of descriptions for the different tabs so that employers know what they are looking at.
- The tab about how an organization can contact providers of certifications and have that resource of all those providers in one place.
- Demographics is nice to see if you are not certain of the type of people you have within a big company.

Meeting with Will Dantzler from CyberKnights

- KSAs has changed to K&S (Knowledge and Skills).
- Individuals can come and take the assessments no matter their role so that organization can have an overlook about their cyber hygiene.
- The organization can then give employees specific trainings that can help their organization have better cyber hygiene.
- HR and IT can work together to meet the new standard of cyber hygiene by using CyberKnights to monitor their cyber hygiene.
- Could possibly have CyberKnights show the tool to an organization.

Appendix C: COSTAR Presentation



Introduction

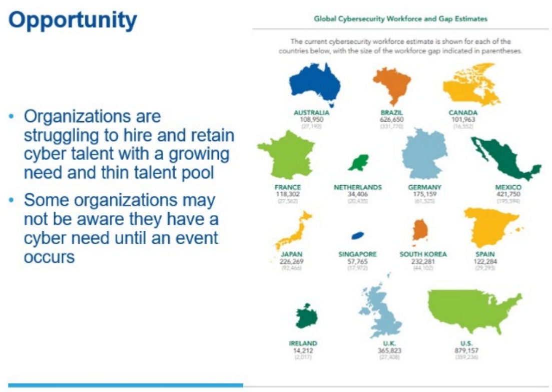
64% of organizations report some form of staffing shortage for dedicated cybersecurity positions

Are you one of them?

Customer

Any organization looking to improving their cyber hygiene

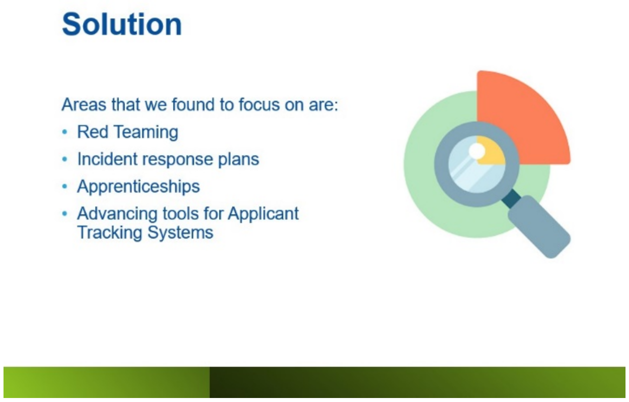
IDAHO NATIONAL LABORATORY



Opportunity

- Organizations are struggling to hire and retain cyber talent with a growing need and thin talent pool
- Some organizations may not be aware they have a cyber need until an event occurs

Global Cybersecurity Workforce and Gap Estimates
The current cybersecurity workforce estimate is shown for each of the countries below, with the size of the workforce gap indicated in parentheses.
AUSTRALIA 108,950 (27,192)
BRAZIL 626,650 (331,770)
CANADA 101,963 (16,552)
FRANCE 118,302 (27,562)
NETHERLANDS 34,406 (20,435)
GERMANY 175,159 (61,525)
MEXICO 421,750 (195,594)
JAPAN 226,269 (92,466)
SINGAPORE 57,765 (17,972)
SOUTH KOREA 232,281 (44,102)
SPAIN 122,284 (29,293)
IRELAND 14,212 (2,017)
U.K. 365,823 (27,408)
U.S. 879,157 (359,236)



Solution

Areas that we found to focus on are:

- Red Teaming
- Incident response plans
- Apprenticeships
- Advancing tools for Applicant Tracking Systems

Team

Human Recourses, IT personnel, Organization Management, Workforce Development personnel from INL

Advantage

- INL has expertise in advancing cyber security
- INL has knowledge about incident response for IT and OT systems
- INL's commitment to diversity brings perspective to this research project

IDAHO NATIONAL LABORATORY

Request/Ask

Do you see any potential problems with this research? Any other feedback?

- Continued opportunity to research the workforce development pipeline for cybersecurity
- Thoughts on focus areas?
- Continue research or develop a specific solution?

WE WANT YOUR
FEEDBACK

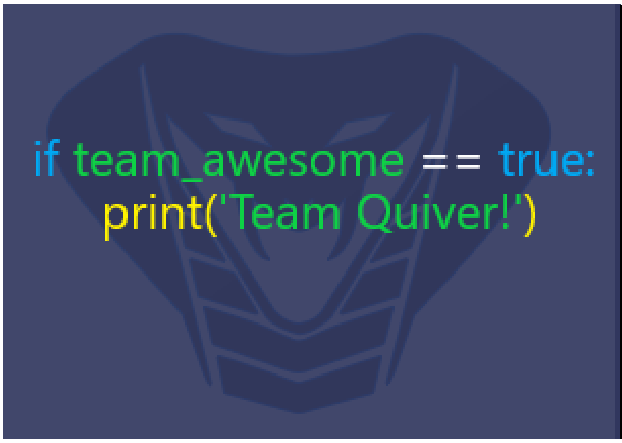
IDAHO NATIONAL LABORATORY

Appendix D: Tasks and Accomplishments

- Research Cybersecurity events that have occurred within the last 10 years
- Research Idaho municipality government and/or State governments
- Review ICRP website and suggest content that could be implemented
- New Interns
- Battlecards created
- Developing surveys to enable businesses to collaborate with INL
- Attended CO*STAR and N&HS Intern Enrichment activities
- New Hire IAA Overview
- Intern Poster Session
- Safety Meeting
- Explored different avenues for solving cohort problem
- Escape room feedback
- Prepared cohort 2 briefing
- N&HS Enrichment Series
- Cyber-CHAMPS Demo
- CyberKnights playground
- Intern Laboratory Director Welcome Event
- Wednesday's IAA Brown Bag
- Started CISA 301V Trainings
- Escape Room Feedback
- Briefed on Cohort Purpose
- CyberKnights Playground
- Intern Laboratory Director Event
- N&HS Enrichment Series
- IAA Brown Bag Enrichment
- CISA 301V Training Completion
- Survey for Companies
- Resume Writing Intern Enrichment
- Cyber-CHAMP Software Development Tasking
- Developing Dashboard for Organizations
- Cyber-CHAMP Demo
- Created wireframes for organizations
- Started development of Dashboard
- Leadership Council meeting
- Completed 301V
- Meet with a manufacturer in Blackfoot
- Started research on apprenticeships
- Question set for organizations
- Research-sharing meetings between Cohorts 2, 3, and 4
- Follow-up meeting with CyberKnights to explore the tool's capabilities

- Attending Cyber Fire Toaster Session
- 401V Training Course
- Meetings with DOL about Apprenticeships
- Discussion with INL HR about Cybersecurity Hiring
- CO*STAR Presentation of Cohort Projects
- Escape Room Collaborations
- N&HS Intern Enrichment Series
- Completed 401v Training

Team Logo:



```
if team_awesome == true:
print('Team Quiver!')
```

Alternate Team Logo: