TECHNOLOGY ASSOCIATION OF OREGON

A Cyber-Studies Strategy for Oregon

Prepared for: Engineering Technology Industry Council

Prepared by: Technology Association of Oregon

May 5, 2014

Document reference No.: TAO-cyber

Cover art: taxedo.com

EXECUTIVE SUMMARY

Objective

This study is intended to assist stakeholders in assessing the feasibility of and identifying considerations for establishing a Center of Cyber-Excellence in Oregon.

Methodology

To better understand the global, national and local factors driving the “skills gap” in cyber-security, this study reviewed published literature, federal programs and news reporting on the subject, reviewed external studies, and conducted an internal survey of local business interests. Additionally the Oregon University System (OUS) provided an internal capabilities survey in the area of cyber education and research to establish a baseline of available educational resources; this baseline was used to evaluate alternative strategies to meet the identified needs in Oregon. The collection and assessment of best practices and lessons learned from other states efforts in this area helped shape variable alternative strategies.

Findings

Establishing a Center of Cyber-Excellence in Oregon is both feasible and practical.

There is an established need within the state for:

- Coordinated curriculum guidelines and recommendations for undergraduate (including Community Colleges) and graduate programs
- Robust continuing education programs (including annual local conferences) to help cyber-professionals remain up to date on their skills.

These efforts must include ongoing dialog with industry to keep these programs and requirements current. The center must include a forward-looking component to assist universities in effectively anticipating next generation educational needs and conducting locally relevant research.

It must be a single, unified Oregon-wide center to maintain required economies of scale and promote cooperation across academic and industry partners.

There is consensus that such a COE can rapidly position itself as the PNW's visionary institution in the area of cyber-security and cyber-education. But there is a difference of opinion as to whether the proposed COE goes far enough – during our drafting discussions with members of the OUS it was suggested that the COE should include a signature research center for cyber-security.

A Cyber-Studies Strategy for Oregon

BACKGROUND

The Technology Association of Oregon (TAO) mission is to have Oregon be a world-class, multi-generational learning ecosystem that prepares all Oregonians to excel in an inclusive, innovation-based economy. TAO helps the region's technology industry to grow through programs and initiatives that focus on industry promotion, advocacy, professional networks, and innovation. In addition, the TAO Foundation serves as a 501(c)3 serving as an "umbrella" non-profit to support educational activities and programs that promote wider access to technology education for Oregon K-12 students. TAO membership includes hundreds of technology and technology-enabled companies from start-ups to established industry leaders, service providers, and government, community and educational institutions.

As part of our outreach we are active in many community panels and advocacy groups. The Oregon University System (OUS) Engineering and Technology Industry Council (ETIC) is an important venue to help ensure postsecondary engineering and technology education in Oregon supports and strengthens the Oregon economy and creates opportunity for all Oregonians. As part of their ongoing assessment of Oregon's needs, the ETIC conducted a cyber-specific education needs assessment in 2013. The assessment titled, "CYBER-CULTURE: An Educational Needs Assessment for the Engineering Technology Industry Council" identified three activities necessary to help clarify the best cyber-excellence strategy for Oregon:

- Market Assessment: With the support of the Technology Association of Oregon in cooperation with ISACA, AOI, OBA, and Oregon Biosciences Association, a survey of Oregon industries was completed in late 2013. The survey was designed to determine the cyber-influenced job functions, titles, certifications and skill requirements required by industry. Additionally, the survey sought to evaluate hiring demand trends, and the level of cyber-competency demonstrated by current candidates for employment.
- Research Assessment: With the support of industry sponsors[i] and the University Deans, ETIC sponsored a round-table discussion to catalog existing cyber-centric research activities, identify synergistic opportunities or research extension to incorporate cyber-centric activity, and qualify the desire and enthusiasm for establishing an Oregon Center for Cyber Excellence.

- Center of Excellence Planning and Analysis: Learning from the successful and unsuccessful strategies in other acknowledged Centers of Excellence, the plan can incorporate best practices that are the most relevant to Oregon's unique needs and capabilities.

Purpose of this Document

To analyze and summarize the three activities above, assess the feasibility of such a center, establish the basis for a formal request of the Oregon State Legislature to fund an Oregon Center for Cyber Excellence, and make actionable recommendations on establishing a Center for Cyber Excellence in Oregon.

CURRENT CHALLENGES IN CYBER-SECURITY

Cyber-security isn't just a computer science issue anymore. As every industry has become dependent on information technology through online presence, social media, data analytics, cloud computing, and electronic commerce, unfortunately, they have also been more at risk from cyber-assault. As highlighted in the most recent FBI Internet Crime Report, the financial impact of cyber-crime is staggering with more than $525 Billion lost in 2012 alone.[ii] It used to be the Federal Government was the only employer of cyber-security experts. Then large international companies found the need to protect their distributed operations from prying entities. Now the need to be vigilant is at all levels from governments to individuals with crime syndicates and individual actors perpetrating cyber-crime in every state, from anywhere [iii]. Cyber-security has become a cost of doing business in the modern age.

CHANGING ENVIRONMENT

There are numerous government and industry-based best practice initiatives underway in support of cyber-security. The Obama Administration created a Comprehensive National Cyber-Security Initiative to integrate the panoply of initiatives promulgated by Federal and law-enforcement needs. The Industry-led Unified Compliance Framework's (UCF) has tried to provide the same type of harmonization of cyber-security compliance objectives. There are a multitude of cyber-security guidelines such as FedRAMP, CAESARS, and SAIR Tier III in the US, as well as numerous international efforts to provide better cyber-security at home and in the workplace. Many of these initiatives and mandates are designed to establish a front line of defense against today's immediate cyber-threats by sharing network vulnerabilities, threats, and events across federal, state, local, and tribal governments, educational institutions and private sector partners in order to act quickly to reduce our current vulnerabilities and prevent intrusions.

A number of NSA and DOD initiatives are designed to defend against the full spectrum of threats by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies. These efforts seek to strengthen the future cyber-security environment by expanding cyber education; coordinating and redirecting research and development efforts; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.

But in light of some of these government-run programs, there comes a recognition that systems have become sufficiently complex and interconnected as to make them not securable. This in turn shifts the mandate from building better walls, to better protecting what is valuable. It used to be we relied on technical measures (and very specialized staff) to protect our critical information. But with the expansive changes in information technology and the revolution in pervasive computing in the last decade the discussion shifted from protection to privacy.[iv] The discussion has played out in many quarters, [v] [vi] [vii] it has fundamentally changed the nature of cyber-security and especially the skills required to be effective in the field.[viii]

PERVASIVE SHORTAGES OF CYBER-EXPERTISE

Addressing cyber-crime requires a skilled workforce trained in the best cyber defenses. For last few years, numerous headlines have shouted about critical shortages of these skilled cyber-experts to combat the surge in cybercrime. [ix] In February this year, the Financial Times had an entire supplement reporting on the current challenges and opportunities in cyber-security[x]. Recruiting remains one of the most pressing challenges both in the United States and across the globe. In the report it is described as both “a big workforce problem” and an “acute skills gap.” More and more firms are turning to automation to help build and maintain a skilled cyber-security workforce. Companies are recruiting new graduates with critical thinking skills and training them in cyber-security techniques to meet their internal hiring needs.

The federal government continues to employ large numbers of cyber-security experts. The Department of Defense expects to increase its own cyber-fighting force to “…more than 6,000 people by 2016, making it one of the largest such forces in the world.” [xi] Defense contractors also employ large numbers of developers and technical staff with cyber-expertise. But the need for cyber-expertise has also been growing in new industries. The Information technology giant HP sponsored a survey of human resources and IT security specialists to “better understand how effective organizations are in hiring and keeping enough skilled and expert staff to meet their IT security mission.” [xii] The study found:

- Most IT security functions are currently under-staffed, but are expected to grow in the next year. On average more than third of staff positions were reported as unfilled in 2013.
- Recruiting and retaining senior security executives continues to be even more problematic than the average. Recruiting takes longer and turnover is more frequent (2.5 years on average).

- On-the-job experience and professional certifications make the biggest difference when hiring a security practitioner. Most job recruiting takes place at conferences.
- By far, salary is the most important part of a hiring package. Competitive salary is the key to stopping turnover.

This is consistent with the industry report as cited in the Financial Times, "*Global demand for people with cyber security skills is forecast to grow at about 13.2 percent each year from 2012 to 2017, according to the Global Information Security Workforce Study by Frost and Sullivan consultants. The 4.2m information security professionals the survey predicts for 2017 will probably be high earners – in 2013, 60 per cent in the sector reporting a salary increase.*"[xiii] The increasing need is creating better opportunities for high wage jobs across a wide-range of industries.

The need for a well trained workforce is both local and global. Oregon has dozens of companies whose operations are directly tied to cyber-security. In addition, state and local government and other government managed critical infrastructure also face significant risk due to cyber-threats. There is an increasing local need for cyber-expertise. There is also the opportunity to draw new business into the area with a highly skilled cyber-savvy workforce. During April 2014, Portland-based Tripwire announced a $12M gift to Pennsylvania State University to aid in the training of the "next generation of cybersecurity leaders." [xiv] This is only the most recent demonstration of Oregon based firms investing in ways to develop the cyber-savvy workforce they need.

FRAGMENTED APPROACHES TO SKILLS DEVELOPMENT AND ASSESSMENT

What does it mean to be highly skilled in cyber-security? Today's job seekers face a conundrum: they are asked to take a battery of extra tests or acquire expensive independent certifications because prospective employers can't easily discern whether "applicants have the right skills" despite having graduated from an accredited program. They can't acquire experience unless they get hired. They wonder why they got their degree. Educators are equally confounded in that they can't build a program to meet a rapidly evolving set of needs in an increasingly wide swath of career fields.

Like many emerging disciplines, the standards of practice are only beginning to be codified. The current state of practice is to hire candidates with solid critical thinking skills and a diploma from and accredited University - and then train them. This emulates the model used by the Federal Government for many years. At the national level, the National Security Agency has had an educational certification program in place since the late 1990s to help address the agency's hiring needs. What is now known as the NSA/DHS Centers of Academic Excellence program certify the curricula of 4 year (and now 2 year) programs as meeting their needs for hiring purposes. Because it is tailored to the skills needed by the Government programs it supports, the program has worked well for them; the program has continued to expand since its inception in the late 1990s and has been revamped with an updated set of evaluation criteria being put in place this year. (For more information on this program see Appendix B.)

Other large employers such as Northrop Grumman and IBM that require a steady supply of new cyber-savvy recruits are also taking a more hands-on approach to getting qualified graduates; they are partnering with local universities directly to specify curricula that better meet their educational needs.[xv] This direct partnership with employers reflects the larger trend of universities moving away from government funding and more to direct or philanthropic sources of investment. It is logical that such a tightly coupled approach would appear in areas of study like cyber-security where hiring remains a challenge. In the cases seen to date the industry partner is local and has a history of hiring from the institution.

But there are emerging alternative models as well. Because the pace of change is so rapid in the cyber-security field a case is being made in some forums to abandon the effort to codify standards and update formal curriculum in favor of a different type of "professionalization": by improving access to knowledge, a wider population can learn the practical, hands on skills needed for everyday cyber-security roles.[xvi] This trend is further supported by the ability of individuals to successfully self-train (through MOOC or other online resources) and secure well-paying jobs in this field. This approach relies heavily on independent certification of testable skills in the field. As mentioned in the HP sponsored study, professional certifications (along with on-the-job experience) "make the biggest difference when hiring a security practitioner." [xvii]

Under either approach, the field has great potential to improve access to better paying jobs through retraining or continuing education. The current mix of approaches has led to a multitude of certifications for specific tools, systems, or areas of risk associated with cyber-security. In addition to general graduate recruiting, hiring managers and Human Resources personnel have had to become experts in validating certification credentials. Some firms do their own testing on site. In the next few years the field may become more defined (professionalized) with rigorous academic or certification standards for some specialized roles.[xviii] But the overall need for more staff with expertise in cyber-security will drive educational needs into many adjacent roles. The need appears to be for more education in a variety of formats and venues: helping people learn the cyber-security skills they need to do their jobs today and continuing into the future.

TAO-ETIC ONLINE SURVEY CAPTURES LOCAL CHALLENGES

TAO conducted a nineteen question survey via Survey Monkey in Fall 2013 in response to the ETIC Education Needs Assessment (see Appendix A for the full findings and results). The survey was designed to assess the current role and import of cyber-expertise in the Oregon business community, collect perceptions of how well the local educational community is addressing these emerging needs, and ascertain trends in the growth of this market need. Key findings include:

Cyber-expertise is increasingly important to and hard to maintain in any organization.

- Cyber-centric expertise such as knowledge of good system infrastructure security design and practices is seen as increasingly important to company operations.
- Companies have multiple positions that require different ranges of cyber-expertise. Staffing these types of positions appears to be problematic. They utilize a multitude of independent cyber-specific certifications in their hiring practices. But the process is made more difficult by a limited local pool of candidates.

Oregon has room to improve in cyber-education.

- More than half of respondents assessed Oregon as having a moderate to significant shortage of “tech talent” today.
- Respondents were only mildly enthusiastic about the availability of recruits coming from the Oregon University System: 38% saw OUS as doing well or very well in meeting their need for qualified candidates, but an equal number saw them as “just okay”.
- In addition to better recruits Companies want access to updated information and research. They appear to be receptive to having access to cyber-centric research and symposiums or conferences hosted by an Oregon institution of higher education on cyber-trends.

- Companies are looking for practical solutions to improving cyber-expertise; they appear willing to utilize continuing education or certification programs via community colleges, tele-education, or other alternative programs.
- The consensus is Oregon is underperforming its potential.

Investment in cyber-expertise expected to accelerate.

- Respondents noted an increasing investment in technical cyber-expertise as well as goods and services requiring those skills. The majority of respondents also expected the overall trend to invest in these cyber-security or cyber-awareness products and services to continue well into the future.

SUMMARY OF CHALLENGES

- The need for cyber-security is becoming an ongoing operating hazard for business and government in Oregon and globally. There are no magic bullets to make it go away.
- Cyber-expertise is increasingly important to a larger number of industries and is hard to maintain in any organization.
- Oregon has room to improve in cyber-education: local employers want practical solutions to improving cyber-expertise and better access to updated information and research. Oregon has an opportunity to increase its performance in a burgeoning market: by employing more Oregonians in cyber-security roles and potentially attracting new firms with cyber-security needs.

LESSONS FROM OTHER CENTERS OF EXCELLENCE

NSA/DHS Centers of Academic Excellence (CAE)

Centers of Excellence have become the moniker of achievement in any technical or highly specialized field. Cyber-security education is no different. The most widely known Centers of Excellence designation for cyber-security is associated with the joint National Security Agency / Department of Homeland Security sponsored National Centers of Academic Excellence in Information Assurance/Cyber Defense (IA/CD) Education Program. The program is designed to encourage the teaching of cyber-security and "growing a pipeline of professionals with information assurance expertise in various disciplines."

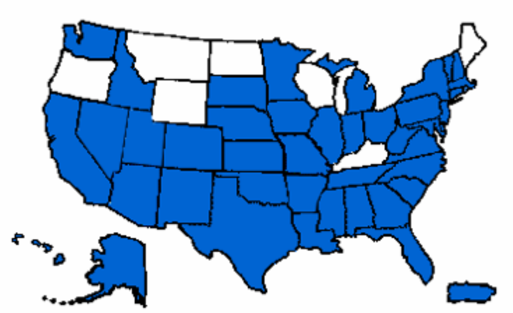


Figure 1: NSA/DHS CAE Program: map showing states with Centers of Academic Excellence in Information Assurance/Cyber Defense. Graphic courtesy of NSA CAE website

The process involved in obtaining the designation is much like a certification program with a minimum essential set of standards. These standards have undergone significant revision in the last two years. The new standards are being put into practice this year. (For additional information about the history of the program and process to apply for CAE designation, see Appendix B.) There are four variants: one for universities or other four-year schools focused on education; another for education focused community colleges or other two-year academic programs; a third focused on universities with research as focal objective; and the fourth focused on providing more tactical (government specific) skills. This diversity reflects the Federal Government assertion that cyber-security is a skill set required for almost any position; it isn't just for computer scientists anymore. The hiring practices of the Federal government have started to utilize the successful completion of two-year certificate program in CAE schools as a competitive differentiator ("preferred qualifications") in hiring decisions.

There are currently over 100 CAEs across the country. **Oregon is currently one of only 8 states without a CAE.** Portland State University discontinued their activity in the program a few years ago and the University of Oregon is currently pursuing CAE status. A full list of CAE institutions is available on the CAE website.[xix] Many schools have cited the designation as a significant boon to recruitment and interest in their cyber-security and related programs. There are also some scholarships available for students interested in Government Service where the designation simplifies the application process.

One of the long stated goals is for the program to have CAEs in every state. They are also looking to "increase in the number of 2-Year Education schools included in the program."[xx] However, the number of hiring entities that use the guidelines is low in Oregon and the surrounding states, possibly because the guidelines are not as well known or as relevant or to the needs of local industry. Certainly for states and schools with a high proportion of graduates looking to be employed in federal positions or government contractors directly connected to cyber-security, the expense of mapping the curricula, applying for, and maintaining the designation is a worthwhile investment in helping their graduates be competitively placed post-graduation. It is an open question about how these designations might be broadly useful in the future in the Northwest, either in placing cyber-security specialists within federal jobs in the area or in providing some starting guidance for curriculum development with an Oregon industry focus.

NSF and other government research funding

The second traditional measure of cyber-security excellence in academia is measurement of research monies awarded to educational institution. While the NSA and the Intelligence Community spend large sums on classified and unclassified cyber-security research, the standard comparative measure for fundamental and applied cyber-research is the peer-reviewed awards from the National Science Foundation (NSF) especially from their Secure and Trustworthy Cyberspace (SaTC) program.

In the last three years, the SaTC program has awarded more than 110 new cyber-security research projects in 33 states, with award amounts ranging from about $100,000 to $10 million.[xxi] A rank analysis (See Appendix C) shows the top ten NSF cyber-security research schools are split equally between CAE and non-CAE status. These schools have made research a priority. The schools are:

1. University of California-San Diego
2. Boston University
3. International Computer Science Institute (at UC Berkeley)
4. Cornell University

5. Carnegie-Mellon University
6. University of Maryland College Park
7. University of Illinois at Urbana-Champaign
8. University of California-Berkeley
9. University of Wisconsin-Madison
10. Virginia Polytechnic Institute and State University

Oregon universities have been successful in competitively awarded cyber-related grants from a variety of Federal and industry sponsors. These awards reflect the capabilities of small teams of world class researchers in cyber-security and related fields. The OUS universities have reported over $8.49M in what they consider cyber-related awards (as detailed in Appendix D) but there is significant potential to expand the capability and better align with local needs.

Industry Measures

On the commercial front entire studies are commissioned to measure the top performing schools in this highly competitive field. These surveys generally take into account both the CAE minimum standards and the more expansive research awards impact. The most recent results of the HP sponsored Ponemon Institute survey (February 2014) cite the University of Texas at San Antonio (UTSA) as the leading school. Their survey of nearly 2,000 security practitioners selected from 403 schools based on perceptions of academic rigor, faculty quality and other measures. [xxii] The list included both institutions who are designated as NSA/DHS CAEs and schools who are not.[xxiii]

The same study highlights the characteristics of these top schools that sets them apart:

- Interdisciplinary program that cuts across different, but related fields – especially computer science, engineering and management.
- Designated by the NSA and DHS as a center of academic excellence in information assurance education.
- Curriculum addresses both technical and theoretical issues in cyber-security.
- Both undergraduate and graduate degree programs are offered.
- A diverse student body, offering educational opportunities to women and members of the military.

- Faculty composed of leading practitioners and researchers in the field of cyber-security and information assurance.
- Hands-on learning environment where students and faculty work together on projects that address real life cyber-security threats.
- Emphasis on career and professional advancement.
- Courses on management, information security policy and other related topics essential to the effective governance of secure information systems.
- Graduates of programs are placed in private and public sector positions.

2014 Ponemon Study:

Top Ten Schools for Cyber-security

- University of Texas at San Antonio (UTSA)
- Norwich University
- Mississippi State University
- Syracuse University and Carnegie Mellon University (tied)
- Purdue University
- University of Southern California
- University of Pittsburgh and George Mason University (tied)
- West Chester University
- U.S. Military Academy at West Point
- University of Washington

from "2014 Best Schools for Cybersecurity," Ponemon Institute LLC, February 2014.

Other Guidance for Oregon from Leading COEs

- **Leverage your unique location -** George Washington University (GWU) made a conscious decision to build their new cyber-security program around their location near the nation's capital. "A lot of what we do hinges on our ability to leverage our connections in Washington."[xxiv] This is similar to the eight community colleges in Maryland (near NSA and DHS) that have sought and obtained the CAE(2Y) designation. Oregon doesn't have that base of Federal cyber-jobs, but it does have cyber-dependent Industries.
- **Don't Confuse NSA/DHS CAE designation with better access to Federally funded cyber-security research.** Research funding is still competitively awarded and CAE designation is not any guarantee or even significant advantage in such competitions.

- The evaluation criteria for the Ponemon survey[xxv] provide an interesting insight to **perceptions of what makes a cyber-security school great**. They include: Academic excellence; Practical relevance; Experience and expertise of program faculty; Experience and background of students and alumni; and Professional reputation in the cyber-security community

These aspects need to be taken into account in developing not only the COE for Oregon but in growing the research and education programs at each of the Oregon institutions.

SUMMARY OF LESSONS LEARNED FROM COES

- NSA/DHS designation as a center of academic excellence in information assurance education is a good independent assessment of the quality of the program. Schools who have achieved the CAE (IA/CD) designation have higher perceived values among both students and employers. But it may not be the right investment for Oregon schools if it isn't used by regional employers.
- Educational programs need to teach critical thinking skills as well as provide hands-on learning environments providing practical skills to address emerging cyber-security threats.
- Diversity is key: ability to attract and maintain a diverse student body with a range of professional interests will lead to the largest impact overall.
- Successful programs teach students of cyber-security management, policy, and other non-cyber skills to help them succeed in their overall careers.

EXPANDING PUBLIC-PRIVATE RESEARCH

Building More Research Relationships in Oregon

Oregon has a number of companies already engaged in cyber-security efforts. These companies already collaborate with and recruit from the Oregon University System. Many of them have active collaborations with or sponsor research at the universities in Oregon. The Center of Excellence should expand these public-private partnerships for the benefit of Oregon. Oregon companies supply a wide variety of products and services across multiple industries all of which require some level of cyber-security innovation or support. University researchers already work for or with industry to develop new technologies and solutions where their expertise specifically addresses company needs. The Center for Cyber Excellence (COE) provides a new vehicle to grow and expand local research partnerships through the development of widely applicable innovative solutions, and delivering a prepared and engaged workforce.

The following is only a partial list of Oregon companies whose operations are directly tied to cyber-security:

ESI
EID
Tripwire
ID Experts
Cambia Health
Kryptiq
EasyStreet
Galois
IBM
Zoomcare
WebTrends
WebMD
Intel
TriQuint
Smarsh
PuppetLabs
Prolifiq
OpenSesame
McAfee
Harris Corp
eBay
Walmart Labs
ShopIgniter
Monsoon
Thetus
Cigna
Lifecome
Kaiser
Providence
Legacy
ADP
The Standard
PGE
Northwest Natural

The COE should make it a priority to support the cyber-security research needs of Oregon based companies and industries. By looking deeply at these local needs, the COE can help industry and academia project technical and educational needs five to ten years down the road. This type of forecasting will help academia better prepare programs and curricula to create a cyber-savvy workforce.

These partnerships will drive economic growth by creating new solutions to emerging problems and supply an educated workforce ready to hit the ground running. Leveraging the local knowledge and contact, the COE can provide a practical framework to ease the challenges of public-private partnerships. In this way location becomes a competitive advantage.

Addressing Real-World Problems

To be useful to Oregon industry, the COE must be able to address the unmet research challenges in industry. Limitations within existing research budgets may preclude necessary infrastructure or equipment needed to effectively address emerging threats. The COE will purposefully invest its resources to expand the effective capacity of the academic organizations to improve responsiveness to well-defined industry needs. We believe complementary investments in innovative workforce training, business support and technology integration assistance are also critical to meeting COE goals.

Initiatives developed by the Center for Cyber Excellence will need to target the elimination of the highest and most common barriers to the successful public private research partnerships in cyber-security. These include:

- Testing and certification – the need to independently validate new solutions and products for industry in real-world conditions.
- Incomplete technology – new discoveries lack critical aspects required for commercialization.
- Sunk cost – the new solutions may be perceived as too expensive but reduced losses in other areas may prove it to be economical from a systems perspective.
- Complex licensing – multiple companies may own portions of the intellectual property needed to bring the material to market.
- Organizational limitations – the new approaches or processes may require new types of research teams, new policies or new competencies not previously mobilized to support its readiness for industry use.

- Workforce – the new processes may require customized workforce training or education.

One way other schools are working to highlight the hands on skills of their students is by sponsoring cyber-challenges with expert judges and Industry sponsored awards. The goal would be to create a network of competitions in Oregon where such realistic challenges become training for regional or national collegiate competitions like the National Collegiate Cyber Defense Competition[xxvi]. Much like the success of robotic initiatives, cyber-challenges can provide much needed opportunity for a largely underserved populations of students to demonstrate applied learning skills.

Easing the Administrative Challenges

The COE structure should provide both the university partners as well as the industry partners an easier way of doing business. Starting with how it is organized and where it locates facilities, each aspect of the COE needs to take into account the needs of both researchers and industry partners. The COE is not designed to replace the existing research relationships but it should enable opportunities for new or expanded relationships. By working together, the investment in education and cyber-education will create better long-term jobs and more opportunities in Oregon.

To help address current administrative challenges the COE will:

- Provide a standardized way to access groups of researchers from multiple universities, including community college faculty, for a single project. The standardized agreements will also support interns from multiple institutions for a single project.

- Take the lead in identifying emerging threats, best practices, and other community-wide cyber-security needs.

- Organize independent testing and evaluation services as needed to support local needs.

- Develop effective information sharing policies to foster productive collaborations. The best solution will be attractive to industrial partners (protecting their proprietary interests), while ensuring wide dissemination of cyber-defense or other best practice information.

- Facilitate better interactions with students throughout their studies; create opportunities for prospective employers to see student's skills at work through internships, competitions, and community outreach.
- Provide a community forum for the cyber-savvy workforce to share best practices and interact through seminars, events, and conferences.

Overall Academic Interest and Engagement with Cyber-security

The COE needs to facilitate the relationships between industry and researchers. To that end the COE needs to reach out to the research community and catalog skills and interests. The COE should provide feedback to the specific institutions as to new skills and expertise that would be useful in expanding the capabilities both within the institution and across the state. A specific goal is to help build a widely used set of academic standards for teaching and assessing cyber-skills across not only computer-science and other "traditional" areas of cyber-study but also the proficiency in cyber-skills appropriate to the study of business, law, education, health management, research, and other increasingly impacted areas of study. As part of their role as intermediary, the COE will collect and identify unmet technical needs in cyber-security from local industry partners; the COE will then share those needs with relevant university researchers and facilitate efforts to create a research partnerships to help address both near term and long term solutions.

Building a Network With Industry Associations

By teaming with Industry Associations the COE can further reduce the barriers to initiating new research. Through meetings and other organized events, the affiliation with Industry Associations also provides opportunities for more personal interactions and relationship building within the cyber-security community. Building up these relationships becomes key to the long-term success of the partnership. Industry Associations already sponsor joint research for its members where there is a common need. This could be expanded, especially if the COE is actively making researchers aware of the emerging needs.

Is a Signature Research Center part of the solution?

Throughout the development of this report the voice of the universities and educators has been sought and considered. There are a number of areas where the universities feel that the COE as presented does not go far enough. For example, they would like to see consideration and funding provided for a Signature Research Center as part of the COE and the addition of 20 new faculty members to support the research and education. There is also the belief that with this Signature Center and growth in faculty that Oregon could aspire to be considered a national leader in cyber-security.

The TAO applauds this aspiration but it is outside the scope of this study. There is reasonable expectation that an Oregon focused COE can rapidly position itself as the Pacific North West's visionary institution in the area of cyber-security and cyber-education. Based on inputs receievd during the course of this study, it is recommended the COE be tasked to work with Industry and the Universities to develop actionable recommendations on how to best expand Public-Private Research in Oregon including examining the utility and impact of creating a Signature Research Center for cyber-security

SUMMARY OF EXPANDING PUBLIC-PRIVATE RESEARCH

- By leveraging existing research relationships and broadening contact through technology and business associations, the overall community of practice can be rapidly expanded.
- This community of practice can be used to help shape and inform the research areas of most utility to local companies.
- The COE can be a coordinating body that helps brings skills and needs together across the local research community.
- The COE can also facilitate research by reducing administrative barriers and investing in common infrastructure and events useful across the community of practice.
- There is an unanswered question as to the best organizing principle to aid multi-institutional research efforts. Creation of Signature Research Center for cyber-security needs to be more fully explored.

IMPLEMENTATION REQUIREMENTS FOR THE COE

Viability of the Proposed COE

There is a measurable need for additional cyber-security experts and overall increase in cyber-expertise across the full gamut of industries in Oregon. Failure of the Oregon University System to address this challenge will result in companies recruiting from farther afield or moving operations to locations with better trained workforces. Alternately, the establishment of an Oregon COE will provide organizations within the state access to research and a qualified workforce. There are many examples of successful Centers of Cyber Excellence in other states. These peer organizations offer ample lessons learned and model approaches to help reduce implementation risk for an Oregon COE. Given the expected increase in need, there should be no shortage of either interested students or research opportunities. Assuming long-term commitment is made to operating the COE, it should be both viable and successful.

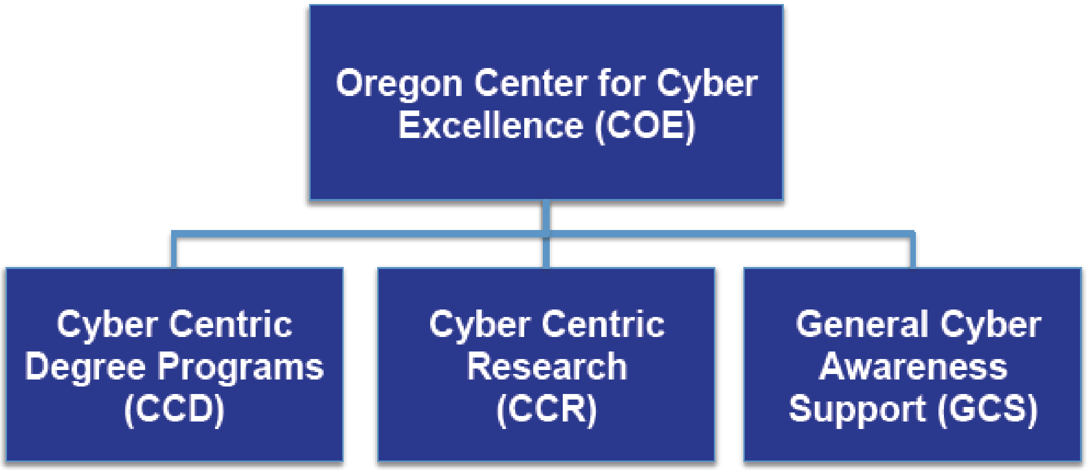
Business Imperatives for the COE

- Provide a necessary service for Oregon: coordinate cyber-security education, share cyber-expertise and disseminate best practices; and facilitate cyber-security research.
- Ensure activities address the breadth and depth of Oregon industries
- Promote cyber-security careers and enhanced cyber-security training for all disciplines.
- Improve cyber-education in Oregon: give local employers practical solutions to improving cyber-expertise and better access to updated information and research.
- Create and execute initiatives to employ more Oregonians in cyber-security roles and potentially attract new firms with cyber-security needs to Oregon.
- Increase the pool of local cyber-savvy workforce candidates.

Organizing Principles

- To make best use of limited resources and provide a neutral coordinating body, create a single Center for Cyber Excellence under the administration of the Oregon University System.[xxvii]

- Increase the capacity within the OUS to ensure the necessary resources exist to build and deliver new Cyber-centric degree programs and engage in key Cyber-centric research efforts.
- Build in economic impact and social impact metrics for all programs. Measure improvements and publish scorecards for all programs.
- Build a diverse workforce.
- Create innovative solutions to cross-cultural and interagency challenges.


Oregon Center for Cyber Excellence (COE)
Cyber Centric Degree Programs (CCD)
Cyber Centric Research (CCR)
General Cyber Awareness Support (GCS)

- Student Readiness
- Certificates
- Community College
- Undergraduate
- Graduate
- Professional degrees
- Continuing Education

- Basic Research
- Applied Research
- Hands-on Classroom
- R&D Support
- Innovation
- Commercialization
- Public Welfare

- Cyber-savvy Workforce
- Community Service
- Workforce Planning
- Community Forums
- Annual Cyber Oregon conference
- Continuing Education

Figure 2: Proposed COE Program Structure

Building Better Cyber-Centric Degree Programs

The COE-CCD will help Community Colleges and Universities build degrees that are more responsive to industry needs. As part of this effort to better increase the effectiveness of the education in helping graduates secure the jobs they seek, the CCD will work with the academic and industry communities to identify the best certification standards and map existing educational coursework to independent certifications to let candidates know when they should be able to take and pass these exams.

CCD will work with local industry to determine if they will utilize the recently updated NSA/DHS CAE criteria in their hiring processes. If they are able to use the designated criteria for discerning quality of candidates, then it would benefit the students for the universities and community colleges to pursue the designation. CCD would then assist the schools in applying for and attaining the NSA/DHS designation as a center of academic excellence in information assurance education. The COE will also help promote understanding of the designation to both students and employers. If local employers do not see utility in the NSA/DHS standards, then CCD will facilitate the development of Oregon-centric standards that do reflect the cyber-skills required by employers in the Northwest. By either path, the goal will be for each institution to have achieved the appropriate cyber-designation by 2018.

The CCD will also work with institutions to ensure educational programs teach critical thinking skills as well as providing hands-on learning environments providing practical skills to address emerging cyber-security threats. They will also encourage teaching students of cyber-security: management, policy, and other non-cyber skills to help them succeed in their overall careers. The CCD will help attract and maintain a diverse student body with a range of professional interests.

Improving Cyber-Centric Research

In addition to better recruits, companies want access to updated information and research. Oregon Universities already play a role in cyber-research but it is limited by the lack of researchers/educators. The COE Cyber Centric Research (CCR) efforts are dedicated to ensuring the cyber-research in Oregon Universities is supporting both the current and future needs of industry as well as the creating opportunities to educate the next generation of cyber-experts. The team will facilitate the initial coordination of the industry partners to include the setting of information, data systems, and operational standards to ensure research conducted in the lab can be easily applied to real-world environments. The COE-CCR will help researchers in both the Universities and in Industry be more competitive and innovative together. Whether it is facilitating an Oregon role in a multi-university research initiative, or helping a university partner with an industry consortium to develop its new discovery into an actionable cyber-defense tool, the COE can play facilitator or mentor role to help Oregon be more competitive. Coe will enable “improved” sharing, enhancing existing university research programs with greater insight and visibility into industry areas of interest. For Industry, the CCR will provide a single point of entry into the university research world easing introductions and helping navigate the administrative hurdles.

CCR will facilitate new research into the emerging cyber-security needs of multi-disciplinary or multi-chain systems. New types of cyber research will involve not only computer scientists but experts from many disciplines. You would expect experts from the business school, medical school and law school to be integral to any conversation about how cyber-threats are affecting data privacy and the acceptable use of personally identifying information (PII) data within their disciplines.

CCR will also assist in having university researchers validate solutions to emerging threats and demonstrate best practices to industry partners as needed. The CCR team would also be chartered to assist in pulling together research experts needed for incident response team needs across the state.

Expanding Cyber-Awareness Education and Outreach

Enhancing other state-wide programs to improve the General Cyber-awareness, the GCS provides the most up to date information and access to cyber-resources across the education spectrum. This team provides a centralized resource for Industry and Government organizations to leverage as needed when questions on cyber-security arise. The GCS team will be responsible for organizing and executing the quarterly “best-practices” meetings as well as annual state-wide conferences on cyber-security education and training. The GCS team in conjunction with the CCR team will be responsible for organizing hands-on cyber-security competitions to promote active demonstration of cyber-expertise and critical thinking skills across all levels of students. The GCS team will include educators as well as program coordinators with skills in event planning, digital media outreach, and stakeholder engagement.

Building on the existing federal and state law enforcement and crime prevention efforts like the Department of Homeland Security “Stop.Think.Connect” program[xxviii] the GCS will translate its expertise on new and emerging cyber-trends developments to provide general cyber-awareness content to other Oregon based offices and programs. This will be accomplished by providing timely and updated information to a full range of Oregon specific channels and venues. The goals are to better prepare the workforce for the challenges of the cyber-age; develop opportunities for volunteers and community driven outreach; and bring insight and expertise regarding cyber-security in workforce planning.

Addressing Stakeholder Needs

Combining the strengths of our education system with industry's needs is a proven combination that pays huge dividends.

For the State: Cyber-centric employment opportunities are knocking; we must answer with an educated work force. This ETIC proposal supports the consolidation and establishment of cyber-centric programs that will support industry's current and future needs. The creation of a Center for Cyber Excellence will not only better prepare Oregon's students for the jobs of the 21st century, but will also enhance our state's economic competitiveness.

For Higher Education: The OUS has a proven track record for creating research institutions to meet challenges and solve problems through discovery, innovation and application. Cyber-research projects offer an opportunity to gain significant new grant funding and develop new areas of collaboration with other leading research institutions. A Center for Cyber Excellence has the potential to create new public-private business partnerships that benefit Oregon. These efforts may also increase the state's profile nationally and internationally in the area of cyber-security and education.

For Industry: More than 100 Oregon companies are directly involved in cyber related commerce. But every Oregon company can benefit from better prepared employee can meet the diverse cyber-centric demands of today's very technically enhanced work environment. Whether the goal is hiring an entry-level office worker or a research scientist, cyber education and training are key ingredients to ensuring Oregon a competitive market edge now and in the future.

For Graduates: Graduates increase their earning potential by developing and refining their capabilities during college. By providing an opportunity for students to focus on cyber-centric jobs students will learn advanced techniques, gain certifications or earn degrees designed to vie for a higher wage. Based on median annual wages, compensation for cyber security professionals ranges from $70,000 to $118,000.

Immediate Next Steps to Validate Scope and Need

- **Collect Best Practices from Peer Centers** - the study team needs to do in-depth assessments of each of the COE peers to best identify the strategies and best practices to implement in the COE. These decisions will be codified in the operating plan for the COE with metrics and provision for periodic reassessment.
- **Refine the Business Imperatives** - The initial TAO/ETIC survey needs to be expanded to better discern regional needs across the state. A survey of prospective students would complement the business survey.
- **Conduct a gap analysis** - based on the information from the peer review and survey results conduct an analysis of resources or structural changes required for the successful implementation of the COE. This would include assessing the need for and cost to establish a Signature Research Center for Cyber-security.
- **Seek support for long term investment** - Identify critical path for funding decisions; formulate budget strategy and secure new term funds to enable rapid startup.

APPENDIX A - TAO/ETIC CYBER-CENTRIC SURVEY

METHODOLOGY

TAO conducted a 19 question survey via Survey Monkey in Fall 2013 in response to the ETIC Education Needs Assessment. The questions were drafted by a roundtable in the late fall with executives from key Oregon cyber-security-related technology firms. Information was requested to identify the current role and import of cyber-expertise in the Oregon business community, collect perceptions of how well the local educational community is addressing these emerging needs, and ascertain trends in the growth of this market need.

TAO members were sent the survey link. The overall response rate was lower than expected (less than 10%) over the multi-day survey window. While the responding population was not statistically relevant, they appear to be representative of the overall pool of TAO member companies with regard to size and industry.

FINDINGS

The diversity of responses appears to reflect the rapidly changing needs in the cyber-security area. Overall responses showed trends in hiring practices and projected needs for Oregon based technology firms. The findings here reflect the depth and breadth of the survey questions. They have been grouped into four basic areas: the role of cyber-expertise in their company, assessment of Oregon cyber-education, a bit of insight about the respondent pool, and cyber-hiring needs and trends.

Cyber-expertise is increasingly important to and hard to maintain in any organization:

- Of the 20 listed cyber centric jobs, each respondent selected an average of 6.4 job categories as important to their organization. Of those, Network Security Engineer and Security Analyst were most prevalent, being selected by 68% of respondents.
- Staffing these types of positions is problematic: 89% of respondents categorized staffing as difficult or very difficult.

- System Infrastructure Security expertise is the most valued at the responding enterprises with 75% of respondents ranking it as first or second. System Infrastructure Audit and Cyber Risk Management expertise were the next most highly ranked skills overall.
- 74% of respondents indicated the listed range of independent cyber-specific certifications as important to critical in their hiring practices today.
- 89% of respondents categorized cyber-centric expertise as important to their company operations.

Oregon has room to improve in cyber-education:

- An overwhelming majority of respondents (95%) predict an increasing need for cyber-expertise.
- 60% assess Oregon as having a moderate to significant shortage of “tech talent” today.
- Respondents were mildly enthusiastic about the availability of recruits coming from the Oregon University System: 38% saw OUS as doing well or very well in meeting their need for qualified candidates, but an equal number saw them as “just okay”.
- Companies want access to updated information and research: two-thirds of respondents indicated their company would be interested in having access to cyber-centric research and symposiums or conferences hosted by an Oregon institution of higher education on cyber-trends. 60% also thought they company would be open to improving cyber-expertise through continuing education or certification via Community Colleges, tele-education, or alternative programs.
- Oregon is underperforming its potential: with regard to cyber-education 60% of respondents rated Oregon as underperforming its potential versus 5% rating it as performing at its potential and 35% who responded “Do not know”.

About the responding population:

- A quarter of respondents work in Information Technology firms; 20% in Banking, Insurance and Finance; 15% in Government and the balance representing Advanced Manufacturing, Healthcare/Medical, Education, Professional Services, and Environmental Technology.

- Company size tended toward the larger - 80% of respondents worked for companies with 100 or more employees.
- Half of the respondents listed themselves as "Management" (IT or Business). The respondent pool also included a high proportion of IT consultants (20%).

Investment in cyber-expertise expected to accelerate:

- General staffing levels are predicted to increase (68%) or not change (26%) in the near term.
- Staffing levels in technical positions requiring cyber-expertise are predicted to increase by 63% of respondents. The same percentage of respondents (63%) indicated "no change" to non-technical positions requiring cyber-expertise.
- 69% of respondents anticipate their company will make investments in new products or services directly associated with cyber-security or cyber-awareness. An even larger number (85%) see the trend for these type of investments increasing in the future.

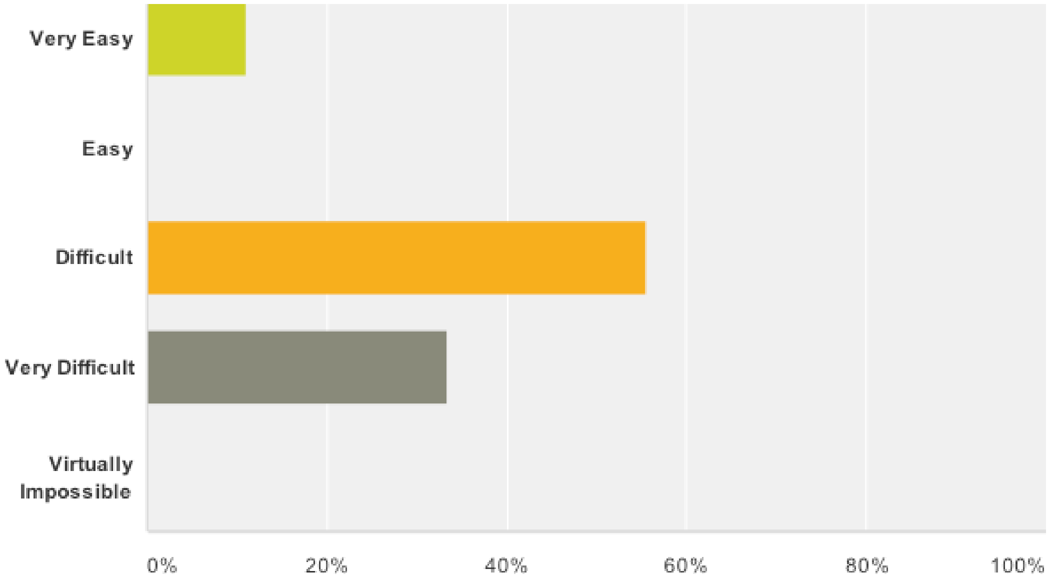
RESULTS BY QUESTION

Q1 SANS has identified the following Cyber-centric jobs, which are important to your organization (select all that apply):

Answer Choices	Count	Percentage
Network Security Engineer	13	68%
Security Analyst	13	68%
Security Architect	11	58%
Security Auditor	**11**	**58%**
Disaster Recovery/Business Continuity Analyst/Manager	**11**	**58%**
CISO/ISO or Director of Security	10	53%
System, Network, and/or Web Penetration Tester	8	42%

Answer Choices	Count	Percentage
Information Security Crime Investigator/Forensics Expert	7	37%
Incident Responder	7	37%
Forensic Analyst	5	26%
Malware Analyst	4	21%
Technical Director and Deputy CISO	4	21%
Security-savvy Software Developer	4	21%
Application Penetration Tester	3	16%
Security Operations Center Analyst	3	16%
Intrusion Analyst	3	16%
Vulnerability Researcher/ Exploit Developer	3	16%
Security Maven in an Application Developer Organization	3	16%
Computer Crime Investigator	0	0%
Prosecutor Specializing in Information Security Crime	0	0%
Total	123	6.4 average

Respondents: 19 answered, 1 skipped



Q2 How easy is it to currently staff for these types of positions?

Very Easy: 2
Easy: 0
Difficult: 10
Very Difficult: 6
Virtually Impossible: 0

Respondents: 18 answered, 2 skipped

Q3 Please rank the following categories of cyber-expertise to your operations:

Answer Choices	1st	2nd	3rd	4th	5th	Average rank
System Infrastructure Security	**8**	7	2	0	3	3.85
Cyber Risk Management	5	3	**8**	3	1	3.40
System Infrastructure Audit	3	**6**	**6**	2	3	3.20
Ecommerce and Personal Information Security	3	2	3	**6**	**6**	2.50
Incident / Data Breach Support	1	2	1	**9**	7	2.05

Respondents: 20 answered, 0 skipped

Q4 There are a number of Cyber-based certifications such as

Cyber Risk Management (GIAC, CAP, CISSP);

System Infrastructure Security (CompTIA, (ISC)2, ISACA, SCP, Q/ISP);

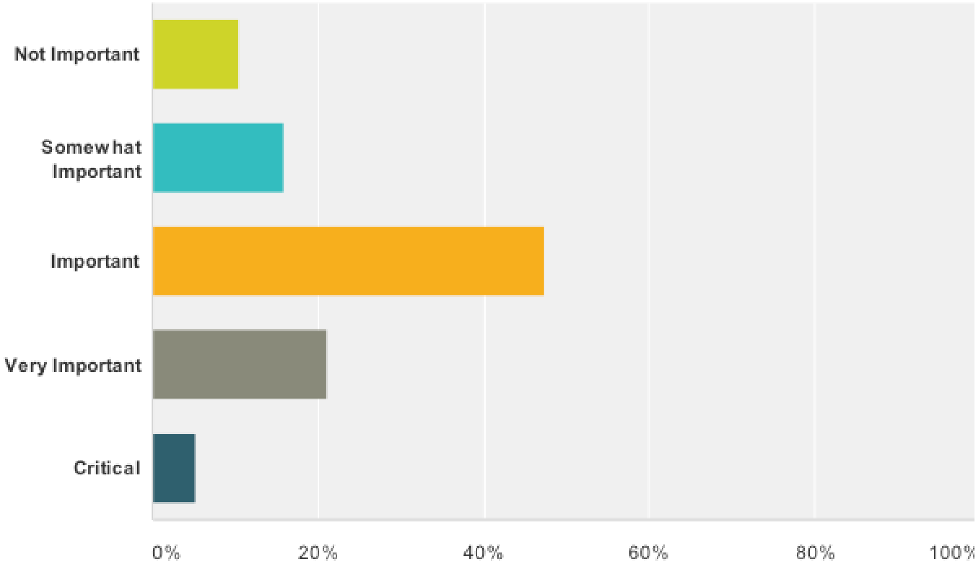
System Infrastructure Audit (ISACA, GIAC, (ISC)2, Q/IAP);

Ecommerce and PII Security (EC, CompTIA, SSCP); and

Incident (Data Breach) Handler (GIAC, DRI, CERT, GIAC).

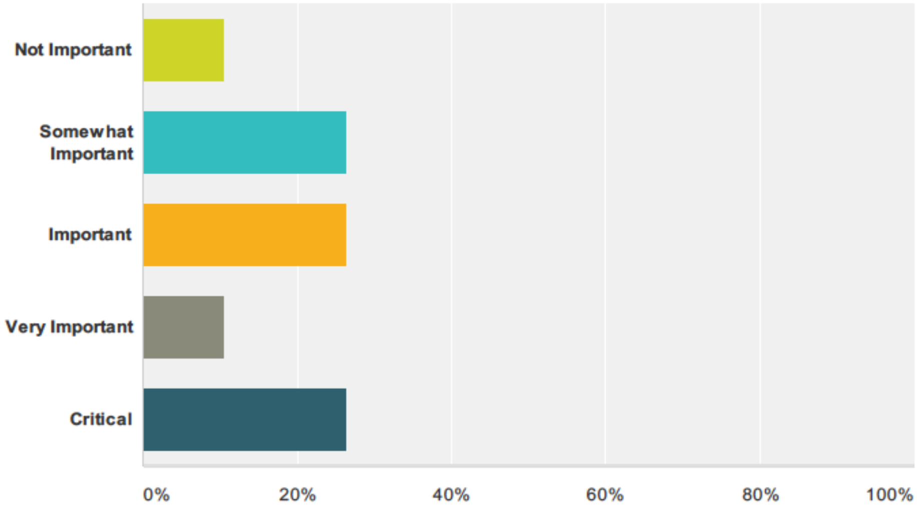
How important are certifications like these for your cyber-centric hires?

Not Important: 2
Somewhat Important: 3
Important: 9
Very Important: 4
Critical: 1



Respondents: 19 answered, 1 skipped

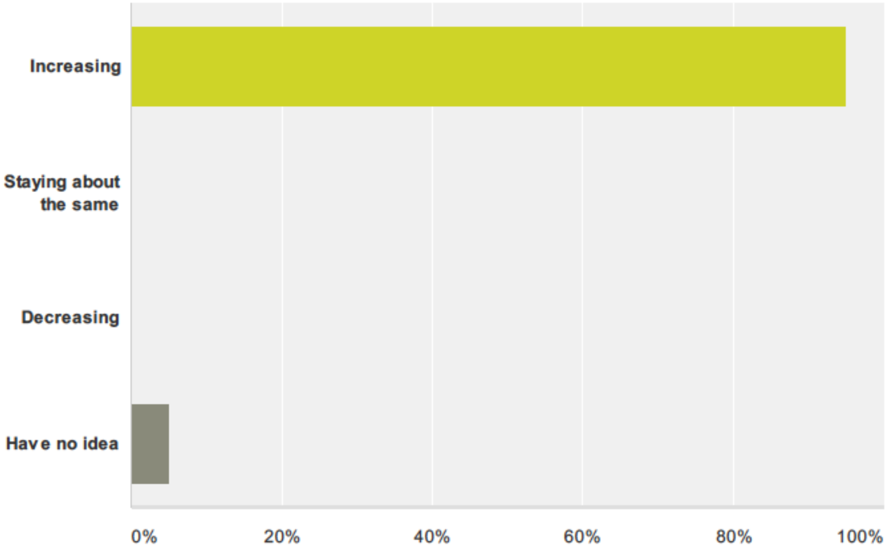
Q5 How important is Cyber-centric (Security, Encryption, Data Privacy, etc.) expertise to the direct operation or the development of to the goods and services provided by your organization?



Not Important: 2
Somewhat Important: 5
Important: 5
Very Important: 2
Critical: 5

Respondents: 19 answered, 1 skipped

Q6 Over the next five years how do you see the need for Cyber-expertise to be trending?



Increasing: 19
Staying about the same: 0
Decreasing: 0
Have no idea: 1

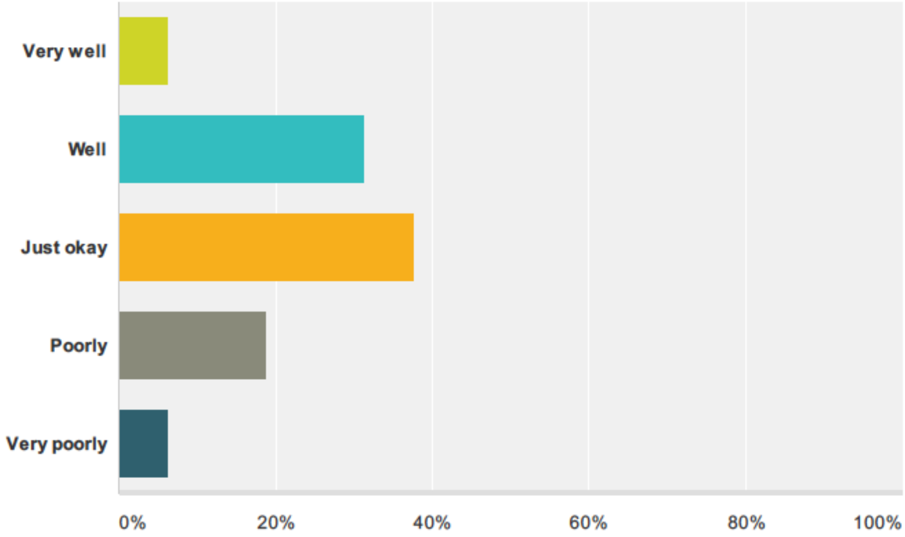
Respondents: 20 answered, 0 skipped

Q7 In general, what is your assessment of the quantity and quality of tech talent in Oregon? Do you think there is a shortage, a surplus, or is the labor market roughly in balance?

Answer Choices	Responses
Significant shortage in terms of the quantity and quality of tech talent	5
Moderate shortage	**9**
Equilibrium, supply of tech talent roughly equals demand	2
Moderate surplus	0
Significant surplus in terms of quantity and quality of tech talent	0
Don't know	4
No Change	0

Respondents: 20 answered, 0 skipped

Q8 Over the past two years, how well has the Oregon University System done in providing qualified candidates to fill your open positions?



Very Well: 1

Well: 5

Just Okay: 6

Poorly: 3

Very Poorly: 1

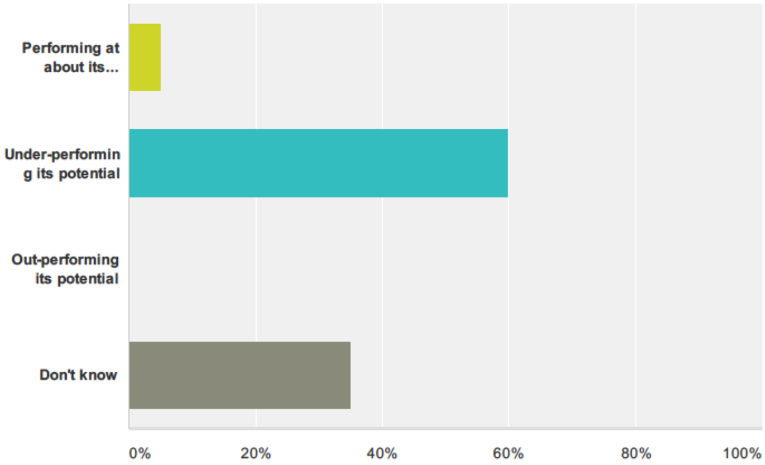
Respondents: 16 answered, 4 skipped

Q9 Which of the following resources would your company use if they were available?

Answer Choices	Responses	Percentage
Access to Cyber-Centric research	**10**	**67%**
Symposiums or conferences hosted by an Oregon institution of higher education on cyber-trends	**10**	**67%**
Community College based continuing education for cyber-expertise or certification	9	60%
Tele-Education options or Alternative programs for cyber-expertise or certification	9	60%
Access to professors who have Cyber-Expertise	5	33%

Respondents: 15 answered, 5 skipped

Q10 Thinking about the Cyber-education, how do you think the State of Oregon is performing relative to its potential?



Performing at about its potential: 1
Under-performing its potential: 12
Out-performing its potential: 0
Don't know: 7

Respondents: 20 answered, 0 skipped

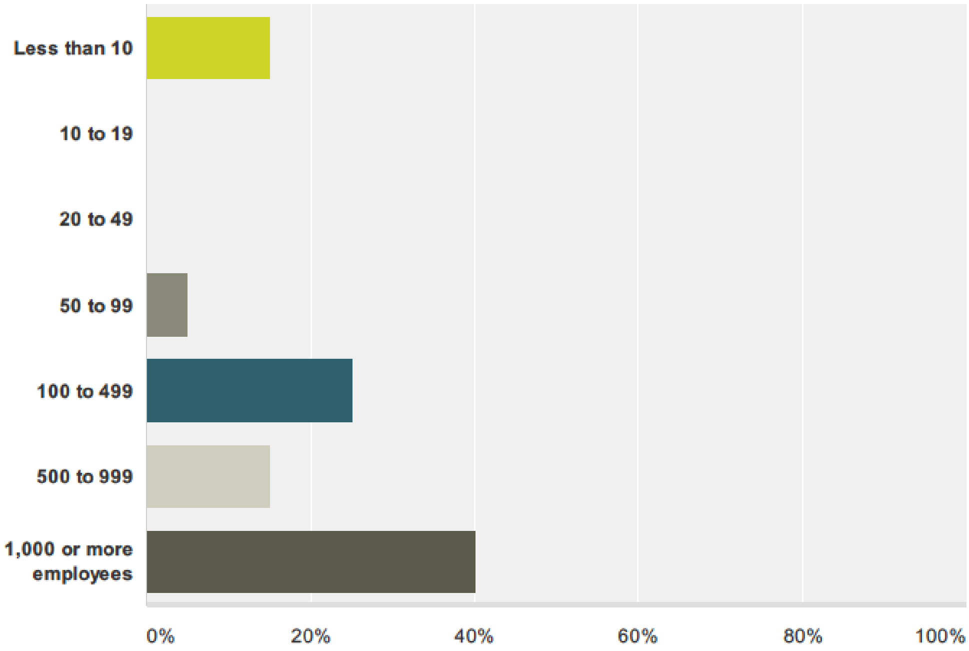
Q11 Primary industry sector for your organization:

Answer Choices	Responses	Percentage
Information technology (IT) or telecommunications	**5**	**25%**
Life sciences	0	0
Advanced manufacturing (non IT sector)	2	10%
Advanced materials	0	0%
Environmental or energy technology	1	5%
Professional services (non IT)	1	5%
Retail/Wholesale	0	0%
Healthcare/Medical	2	10%
Financial/Banking/Insurance	4	20%
Media/Publishing/Entertainment	0	0%
Government (federal, state, local)	3	15%
AMTUC (Agriculture, Mining, Transportation, Utilities, Construction)	0	0%
Education	2	10%
Hospitality/Food/Beverage	0	0%

Respondents: 20 answered, 0 skipped

Q12: How many total employees does your organization have?

Respondents: 20 answered, 0 skipped

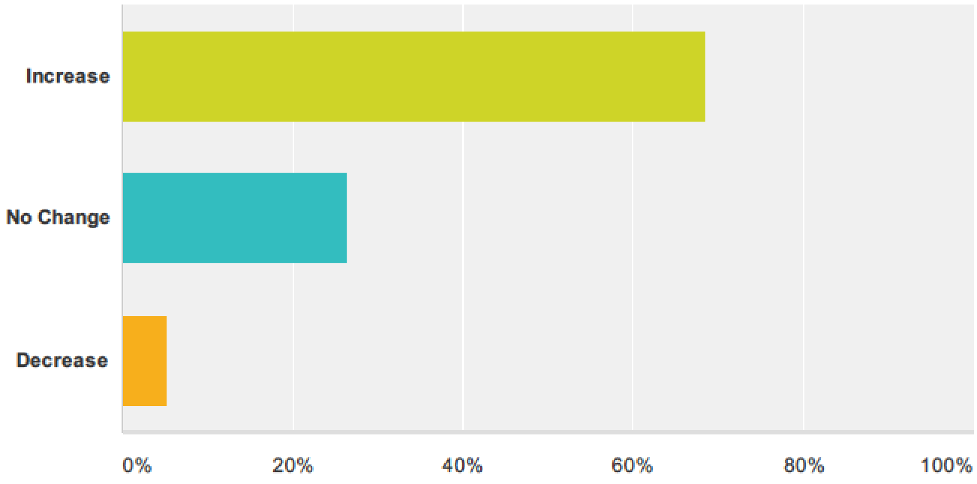


Q13 Which of the following best describes your position?

Answer Choices	Responses	Percentage
Senior Executive (CEO, President, Owner, etc.)	0	0%
Executive - IT function (CIO, CTO, VP or equivalent)	2	10%
Executive - Business function (CFO, CMO, COO, VP or equivalent)	1	5%
Management - IT function (Director, Manager, Team Leader etc.)	**5**	**25%**
Management - Business function (Director, Manager, Team Leader etc.)	**5**	**25%**
Staff level - IT function	3	15%
Staff level - Business function	0	0%
IT Consultant	4	20%
Business Consultant	0	0%

Respondents: 20 answered, 0 skipped

Q14: A. General Staffing Levels



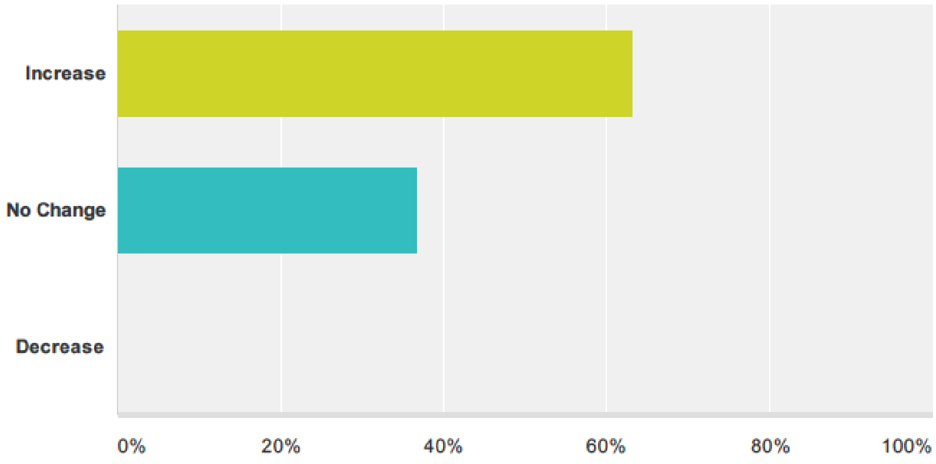
Increase: 13

No change: 5

Decrease: 1

Respondents: 19 answered, 1 skipped

Q15: B. Staffing levels in technical positions requiring Cyber-Expertise?



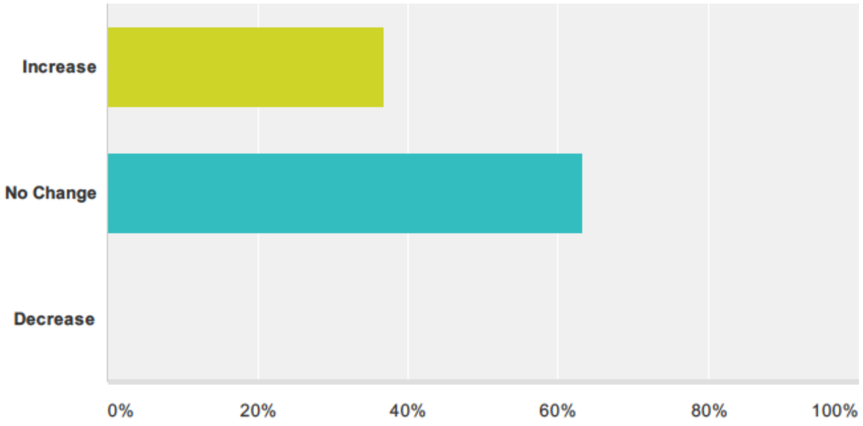
Increase: 12

No change: 7

Decrease: 0

Respondents: 19 answered, 1 skipped

Q16: C. Staffing levels in non-technical positions requiring Cyber-Expertise



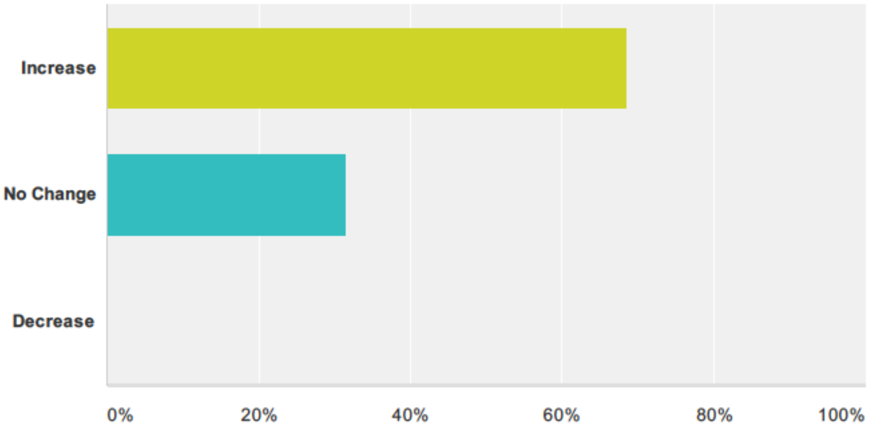
Increase: 7

No change: 12

Decrease: 0

Respondents: 19 answered, 1 skipped

Q17: D. Investments in new products or services directly associated with Cybersecurity or Cyber-awareness?



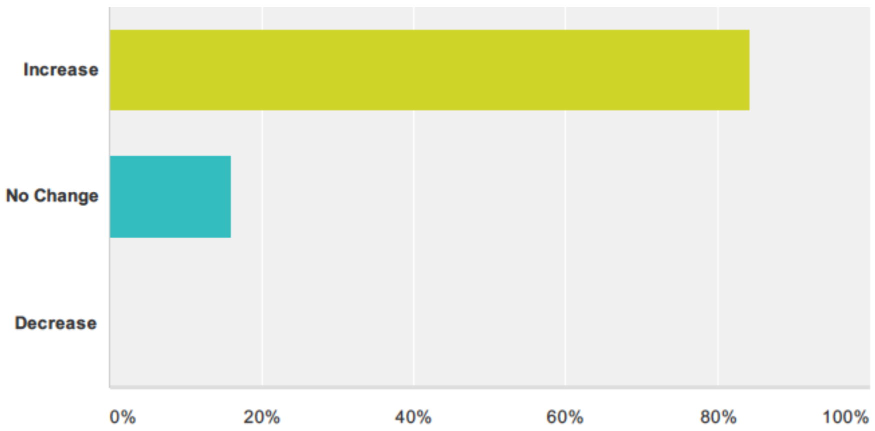
Increase: 13

No change: 6

Decrease: 0

Respondents: 19 answered, 1 skipped

Q18: E. What do you see as the trend for these types of Cyber-Investments in the future?



Increase: 16

No change: 3

Decrease: 0

Respondents: 19 answered, 1 skipped

Q19 Please provide any comments or feedback:

Respondents: 3 answered, 17 skipped

APPENDIX B - NSA/DHS CAE PROGRAM INFORMATION

Background on the NSA/DHS Center of Academic Excellence (CAE) Programs

"The National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence (CAE). The goal of CAE is to reduce vulnerability in our national information infrastructure by promoting higher education and research, and producing a growing pipeline of professionals with information assurance expertise in various disciplines."

Originally a NSA driven program designed to facilitate recruiting skilled graduates and facilitating excellence in research. The program is currently a supporting component of the National Initiative for Cybersecurity Education for Workforce Training and Professional Development.

The program is currently known as National Centers of Academic Excellence in Information Assurance/Cyber Defense (IA/CD) Education Program. They currently offer CAE designation of three types: Excellence in IA Education (CAE/IAE), IA 2-year Education (CAE/2Y) and IA Research (CAE/R) programs. All regionally accredited two-year, four-year and graduate level institutions in the United States are eligible.

CAE PROGRAM HISTORY

1998 – first competition based on CNSS criteria

1999 – First seven centers are awarded.

2003 – DHS becomes a co-sponsor of the program,

2008 – Addition of the Research (CAE/R) designation

2010 – Inclusion of Community Colleges

There is also a program for CAE-Cyber Operations open to academic Institutions. The program is similar on nature and process to the CAE/IA programs but is focused on "technologies and techniques related to specialized cyber operations (e.g., collection, exploitation, and response), to enhance the national security posture of our Nation. These technologies and techniques are critical to intelligence, military and law enforcement organizations authorized to perform these specialized operations."[xxix]

The process previously involved mapping courseware to the Committee on National Security Systems standards. But the process has been re-designed in response to feedback from the academic community. The core criteria have been re-mapped to "Knowledge modules" and the new criteria are in place beginning with the 2014 competition.

"The retooling of the joint National Centers of Academic Excellence program includes the elimination of dated, controversial federal training standards. They are being replaced with curricular blocks, dubbed "knowledge units," that officials say will enable colleges to develop cybersecurity focus areas while also allowing them to respond to employers' needs in a fluid marketplace."[xxx]

The Current Program

Updated Criteria for CAE-2Y, CAE, CAE-R, CAE-OP Designation are available on the temporary (transitional) website.[xxxi] New applications can be submitted throughout the year. The process is very much like an accreditation or proposal process. The application form and guidelines are available online. Institutions collect, write and submit documentation on how their curricula map to the "Knowledge units". Quite similarly to an accreditation process, the package of materials is reviewed and evaluated for compliance and adequacy. Assuming the collective package meets standards, the designation is awarded.

Once unique feature of the program is assignment of a liaison to work with the partner institution.

> "The IA mission at NSA assigns a Security Education Academic Liaison (SEAL) representative to each of the National Centers of Academic Excellence in IA Education (CAE/IAE) and National Centers of Academic Excellence in Research (CAE-R). These representatives promote collaboration between the government and universities, define areas of mutual interest, and identify sources for research and development. Of particular interest to both is the identification of outstanding students for future government employment."[xxxii]

The Debate About Excellence

A bit of history from the start of the program and its “devolvement to adequacy[xxxiii]”

In his well-read blog post, Dr. Spafford (Spaf) at Purdue University, one of the researchers involved with the initial development of the program has opined about program and its devolvement to adequacy. His primary objections are:

- In meeting the program’s goal of encouraging universities to teach about cyber-security and information assurance, they have devalued the term “Center of Excellence” as a mark of superlative achievement. His opinion is there can’t be 100+ centers of equal excellence in a dynamic field.
- “CNSS standards are really training standards, and not educational standards.” The current revamp of the program into Knowledge Modules is designed to better address this concern, but the initial press has been mixed.
- The intended “exclusivity” of the access to additional resources has not materialized. “The Scholarship for Service program is open to non-CAE schools.” This is still true with the 2014 program announcement. See note below.

> In the words of Dr. Spafford, “Instead of actually designating excellence, the CAE program has become an ersatz certification program. The qualifications to be met are for minimums, not for excellence. In a field with so few real experts and so little money for advanced efforts, this is understandable given one of the primary goals of the CAE program -- to encourage schools to offer IA/IS programs. Thus, the program sets a relatively low bar and many schools have put in efforts and resources to meet those requirements. This is a good thing, because it has helped raise the awareness of the field. However, it currently doesn't set a high enough bar to improve the field, nor does it offer the resources to do so. Setting a low bar also means that academic program requirements are being heavily influenced by a government agency rather than the academic community itself. This is not good for the field because it means the requirements are being set based on particular application need (of the government) rather than the academic community's understanding of foundations, history, guiding principles, and interaction with other fields. (e.g., Would your mathematics

> department base its courses on what is required to produce IRS auditors? We think not!) In practice, the CAE program has probably helped suppress what otherwise would be a trend by our community to discuss a formal, common curriculum standard. In this sense, participation in the CAE program may now be holding us back."[xxxiv]

Relationship to "The Scholarship for Service" program

One of the explicit goals of the CAE process is to attract students into government cyber-service. A specific offshoot of the Federal Scholarship for Service program is tailored for students studying in areas of cyber-security. Under this program the educational institution can apply for a block grant of scholarships. The competitive grants, if awarded, allow eligible students at the Institution scholarships in exchange for agreeing to work for the government for a defined period of time after graduation. The Institution does not have to be a CAE to be eligible. However being a CAE makes the submission paperwork a bit easier. Non-CAE Institutions have to provide "equivalent evidence documenting a strong program in cybersecurity." [xxxv]

Current Program Goals

"NSA and DHS also plan to continue to build the relationship with CAE in fiscal year 2013, pursuing a long-term goal of reaching all 50 states at the program's optimized point. NSA and DHS would like to see an increase in the number of 2-Year Education schools included in the program."[xxxvi]

APPENDIX C - Analysis of NSF funding

METHODOLOGY

In an effort to better understand the linkage between cyber-security research and education analysis was conducted on the National Science Foundation (NSF) funding data set for cyber-security studies. The data is from the NSF's interdisciplinary Secure and Trustworthy Cyberspace (SaTC) program. The SaTC data published by the NSF represents over $185M investment over the last three years. It consists of 449 awards to 133 entities. The entities are primarily universities with a handful of nonprofit and for profit companies.

The data set includes:

Internal NSF references: NSF Award Number, NSF Organization (managing organization), NSF Program (group) name, NSFDirectorate, ProgramElementCode(s), ProgramReferenceCode(s)

Funding information: Start Date, LastAmendmentDate, AwardInstrument, ExpirationDate, AwardedAmountToDate, ARRAAmount (none of these have ARRA amounts)

Performer information: PrincipalInvestigator, State, Organization, ProgramManager, Co-PIName(s), PIEmailAddress, OrganizationStreet, OrganizationCity, OrganizationState, OrganizationZip, OrganizationPhone

Project specific information: Title and Abstract of the project

Three measures in the file were averaged to arrive at a final ranking. The three elements used were proxies for the overall size, scope, and competitiveness of the program:

- Total Award Value (data element: Sum of the Amount awarded to date) - used to gauge overall size of their cyber-security research program.
- Total Count of awards by Organization (data element; strict summation of count by Organization name field) - used to assess the overall competitiveness of the program based on number of awards competitively awarded.
- Average value of awards by Organization (data element Division of Total Award Value above by Total Count above.

ANALYSIS

Total single award values ranged from $5,000 (student support grants) to over $5 million (ActionsWebs theory research at University of California, Berkeley); by awardee values ranged form $10,000 (Association of Computing Machinery) to $9.8M (Carnegie Mellon University.) Carnegie Mellon also had the highest number of awards at 20; 52 awardees had only one award. Average award size ranged from 10,000 (Association of Computing Machinery) to $1.5M (University of California, Berkeley)

It is interesting to note in addition to the University of California, Berkley being listed as an awardee, an affiliate the International Computer Science Institute (ICSI) is ranked higher. ICSI is an independent, nonprofit Computer Science research institute established in 1988.

For this analysis we are looking for good examples of robust, sustainable cyber-security research programs within education oriented entities. The top ten awardees by weighted ranking (listed below) provide a good set of candidates for further assessment for actionable insights on how to build similar high-functioning programs in Oregon.

Oregon's three listed schools rankings are listed for comparison at the end of the table.

Top ten NSF Cyber-security (SaTC) Funded Awardees by weighted average.

	School	Total Awarded $M	Award Count	Average award $k	DHS/ NSA CAE	$ rank	count rank	avg $ rank	final rank factor
1	University of California-San Diego	$8.8	13	$678	none	2	2	9	4.33
2	Trustees of Boston University	$6.0	8	$756	IAE, R	3	10	7	6.67
3	International Computer Science Institute	$5.3	7	$763	none	6	15	5	8.67
4	Cornell University	$4.5	8	$572	none	7	9	11	9.00
5	Carnegie-Mellon University	$9.8	20	$492	IAE, R	1	1	31	11.00
6	University of Maryland College Park	$4.3	8	$537	R	9	12	18	13.00
7	University of Illinois at Urbana-Champaign	$5.9	13	$452	IAE, R	4	3	40	15.67
8	University of California-Berkeley	$5.9	4	$1,464	none	5	43	1	16.33
9	University of Wisconsin-Madison	$3.4	6	$567	none	13	25	12	16.67
10	Virginia Polytechnic Institute and State University	$3.3	6	$556	R	14	26	15	18.33
39	Portland State University	$1.6	4	$408	none	43	42	52	45.67
78	University of Oregon Eugene	$0.6	4	$152	none	68	45	117	76.67
128	Oregon State University	$0.1	1	$52	none	130	102	130	120.67

APPENDIX D OUS CYBER-RESEARCH INVENTORY

CONTEXT

In conjunction with the study being done by the TAO, representatives from OSU, UO and PSU held a number of planning meetings to identify areas of cyber-security research and education which would be required to make the efforts of an Oregon COE successful.   As an initial step, they created an inventory of current research and education activities focused on cyber-security. The inventory documents the number and variety of ongoing cyber-security related research activities underway across the OUS.

Of the 26 awards provided: 16 were at University of Oregon for a total award value of approximately $3M; six awards were at Portland State University for a total award value of $2.8M ; and 4 were at Oregon State University for a total award value of $2.7M. These awards include projects funded under the NSF SaTC program detailed in the previous section but also a mix of government and industry sponsored projects. Government sponsors include: DHS, Defense Advanced Research Projects Agency (DARPA) and the Army Research Office (ARO). Industry sponsors inlcude companies like Intel, Google and Narus. These awards are across a small number of researchers and represent a relatively modest percentage of the total sponsored research at any of the three universities.

Current OUS Cyber-security Research

Oregon State University	Sponsor	Grant
Detecting insider threats in organizations.	DARPA ADAMS Program	$1.67M
Diversity & Feedback in Random Testing for Systems Software	NSF	$242K
CAREER: Integrated Automated Software Testing Methods	NSF	$400K
CAREER: Secure Computation	NSF	$400K

Portland State University	Sponsor	Grant
Cyber-Discovery Camp at PSU	NICERC/DHS	$153K
Increasing the Cost of Malware	NSF SaTC	$498K
CAREER: Design Principles for Cryptographic hash Functions: foundations, Primitives, and Transforms	NSF SaTC	$400K
Theory and Practice of Tweakable-Blockcipher-Based Cryptography	NSF SaTC	$433K
SOUND: Safety on Untrusted Network Devices	DARPA MRC	$1.02M
Trustworthy Hardware from Certified Behavioral Synthesis	NSF SaTC	$299K

University of Oregon	Sponsor	Grant
Student Travel Support for the 21st IEEE International Conference on Network Protocols (ICNP)	NSF	$15K
Supporting Student Travel to 2013 ACM Conference on Computer and Communications Security (CCS 2013	NSF	$10K
Network traffic analysis and characterization	NARUS Inc.	$40K
NeTS: Small-Buddyguard—A Buddy System for Reliable IP Prefix Monitoring	NSF NeTS	$300K
CAREER: A Behavior-Based Framework for Detecting Internet Worms	NSF CT	$426K
NeTS-NBD: Internet Routing Forensics—A Framework for Understanding, Monitoring and Detecting Abnormal Border Gateway Protocol Events	NSF	$378K
Automatic Defense Against Unknown, Self-Propagating Worms Using a Distributed Monitoring System	Intel	$87K
Planetlab—academic nodes	Intel	$9.4K
Provenance-based Access Control	MIT Lincoln Labs	$75K
CAREER: Securing Critical Infrastructure with Autonomously Secure Storage	NSF	$400K
Oregon Security Day	NSF	$8K
BGP Security Study	Battelle	$60K
TC: Small: Protection Methods for Portable Storage	NSF	$500K
Characterizing and Implementing Efficient Primitives for Privacy-Preserving Computations	DOD/DARPA	$375K
Learning Tractable Graphical Models with Latent Variables	Google	$57K
A Unified Approach to Abductive Inference	ARO	$233K

Key Research & Education Areas in Support of an Oregon COE

In discussing cyber-security related research, representatives from UO, OSU and PSU identified a number of forward looking cyber-security related areas where the universities could contribute as both researchers and educators. These key focus areas of interest leverage existing organizational expertise and experience but pose significant research challenges. Each research area is seen as critical for the success of an Oregon COE and Oregon industry. The COE should facilitate a discussion among the Oregon cyber-security community of practice to determine local interest in the following areas of research interest.

Key Focus Areas for Cyber Security Research

- Improved Internet Privacy and Security
- Ensuring privacy and security in the Internet of Things
- Addressing the unique challenges of securing “Big Data” (Privacy and Security)
- Smart Grid Security and Availability

Research leads to New Education Programs and Offerings

The success of an Oregon COE will be dependent on OUS growing the capacity and depth to build and deliver new educational programs as well as build research depth in areas critical to Oregon industry. Expansion of traditional classroom based courses requires hiring additional faculty or lecturers at both the Universities and Community Colleges. The introduction of new, hands-on or practical curriculum requires a larger number of faculty per targeted student to ensure the correct supervision in a more lab-oriented environment. The type and expertise of faculty also becomes more specific in these types of courses. Faculty will be more research oriented and require investment in new teaching labs and equipment.

Areas for the COE to explore further with researcher-educators include:

- Hands-on programs to engage students early and throughout their education to bring students into Cyber-security programs.
- Practical Continuing Education offerings in Cyber-security for working professionals.
- Tailored Cyber-security Degree and Certificate Programs

Based on conversations with the representatives from the Universities, an estimated 20 additional faculty may be needed across the universities to fully execute the education strategies discussed in this study. An equal number of new faculty or lecturers may be needed across the Community Colleges to address the Continuing education and certificate program needs.

The COE should be tasked with better defining the new paradigm of teaching cyber-security; the impact of infusing cyber-relevant content into other study areas such as law, medicine, and business; and the best way to measure readiness across skill sets.

APPENDIX E - OREGON COE PEER GROUP

CONTEXT

There are many Centers of Excellence in cyber-security across the country. Each one is a little different, reflecting its unique capabilities and history. As part of the process of determining how to best establish a Center for Cyber Excellence in Oregon it is good to look more deeply at a small number of relevant examples. It is expected that a small team of educators and administrators would contact the selected aspirational peers and develop longer term relationships for the purpose of obtaining insights, lessons learned and best practices for an Oregon based COE.

For this analysis we have split the selections into two categories, roughly approximating the split between Community Colleges (two year programs) and Universities (four year programs) including Research-intensive programs.

Community College Aspirational Peers are drawn from the 32 current NSA/DHS IA/CD CAE (2Y) designated schools listed below:

- Alabama - Snead State Community College
- Florida - Florida State College at Jacksonville and Valencia College
- Hawaii - Honolulu Community College
- Illinois - Moraine Valley Community College
- Indiana - Ivy Tech Community College
- Louisiana - Bossier Parish Community College
- Maryland - Anne Arundel Community College, College of Southern Maryland, Hagerstown Community College, Harford Community College, Howard Community College, Montgomery College, Prince George's Community College, The Community College of Baltimore County
- Minnesota - Inver Hills Community College and Minneapolis Community and Technical College
- New York - Erie Community College
- Ohio - Owens Community College and Sinclair Community College

- Oklahoma - Francis Tuttle Technology School, Oklahoma City Community College, Oklahoma Department of Career & Technology, and Rose State College
- Tennessee - Jackson State Community College
- Texas - Richland College of the Dallas County Community College District, San Antonio College, and St. Philip's College
- Virginia - Northern Virginia Community College
- Washington - Highline Community College and Whatcom Community College
- West Virginia - Blue Ridge Community and Technical College

To get the best mix of insight from these leaders in the CAE 2Y community. It is recommended the planning group contact the following groups to obtain lessons learned and advice on how to best implement a program Oregon-wide for interested Community Colleges to have their cyber-security endorsed under the NSA/DHS IA/CD Center of Academic Excellence (2Y) program:

- **Prince George's Community College (CyberWatch Lead Institution)** - The Cyberwatch[xxxvii] program was one of the driving forces behind the 2Y certification. Located quite near NSA headquarters, in PGCC-CyberWatch has also developed a reputation for mentoring other 2-year institutions who wish to apply[xxxviii]. Mt. Hood Community College (Oregon) is already a member of the CyberWatch organization. PGCC has valuable insights as to how to co-develop standards for a certification program and experience with building and expanding a base of support in their community.
- **Moraine Valley Community College (CSSIA Lead Institution)** - The Center for Systems Security and Information Assurance ([xxxix]CSSIA) is a National Science Foundation (NSF) Advanced Technological Education (ATE) National Resource Center. Located in Palos Hills, Illinois CSSIA is another of the first round of two year programs selected. They are also known to provide lessons learned and other resources to prospective applicants. A bit different in local needs than PGCC, MVCC is committed to supporting industry specific needs in the greater Chicago area with an interesting focus on career readiness.

Additionally the groups should develop a relationship with the two Washington based CAE (2Y) institutions - **Highline Community College** and **Whatcom Community College.** Like Highline

Community College, **Honolulu Community College** earned its designation in 2013, so they would have the most recent experience about going through the process. These schools will have similar regional needs as those in Oregon. Each are far from the pools of government jobs that seem to be the focus of many of the other CAE (2Y) programs.

University Aspirational Peers are drawn from the HP study (Industry) Top Ten as discussed previously as well as the top NSF cyber-research performers as measured by weighted average (Appendix C). The recommendation for aspirational peer schools to study in more detail are a targeted subset of the two lists. The recommended schools are:

- **Carnegie Mellon University** - The only school to be on both lists. It has a long history of work in the field. They are also currently have NSA/DHS IA/CD designations for both Information Assurance education (IAE) and Research (R). With a core cyber-security focus in the School of Computer Science, Carnegie Mellon has been at the forefront of cyber-security research especially “Trustworthy Computing” for more than two decades. They are offering some interesting cross-discipline Masters programs including eBusiness Technology and Privacy Engineering[xl].
- **University of Texas at San Antonio (UTSA)** - The top scoring school in the HP survey. UTSA’s College of Business is one of the leading institutions in the field of infrastructure assurance education. They have both the IAE and R designations. While it also has more traditional research, UTSA’s distinguishing program is their approach to teaching cyber-skills in their College of Business: “Within the College of Business more than 150 students major in cyber security at the undergraduate, masters and doctoral levels. Students learn how to protect data, gather and examine digital evidence, perform security risk assessments and study computer and network forensics procedures.” [xli] Their approach may provide significant insight in how to teach cyber-security for the start-up and micro-company community in Oregon.
- **University of California-San Diego** - The top scoring school in the NSF funding analysis. They have built a more traditional Computer Science driven program. They do not currently participate in the NSA/DHS CAE program. Their model is departure from the others on the list, but they continue to be very successful. They have branched into super-computing, data security and other approaches that assist the emerging local biotech companies.

- **International Computer Science Institute / University of California, Berkeley** - Two of the top scoring awardees in the NSF funding analysis. They are included because they have been very successful without the CAE designation and have a unique, apparently supportive relationship for a cooperative public-private model for cyber-research.

- **University of Washington** - The only northwestern University on the HP top ten list. The Center for Information Assurance and Cybersecurity (CIAC)[xlii] describes their interdisciplinary approach as a "unique collaboration between information science, computer science, economics, electrical engineering and law."[xliii] They have had their IAE designation since 2004 and their Research designation since 2008. Their model provides a very Northwest-centric approach to delivering cyber-expertise to the region and has significance for an Oregon based COE.

APPENDIX F - PROPOSED COE IMPLEMENTATION PLAN

INTRODUCTION

A unique opportunity exists in the Oregon cyber-security community today; by virtue of how the state has developed over the years and with consideration for the immense investment by the business community, Oregon has a unique opportunity to collaboratively create the next generation, cyber-savvy workforce. As outlined in the ETIC needs assessment, “CYBER-CULTURE: An Educational Needs Assessment for the Engineering Technology Industry Council” and corroborated by the TAO sponsored survey of employers Oregon needs to rapidly increase the number of cyber-savvy workers and the current educational approaches are not fully addressing the need.

By leveraging current best practices across educational organizations and adding in innovative approaches to address unmet needs, Oregon education can play a larger (and perhaps unique) role in creating the cyber-ready workforce desired by Industry.

Known for taking a more collaborative approach, Oregon education and industry partners have an excellent track record of bringing together excellent academic and private researchers, and improved facilities from across the state to meet specific objectives. An Oregon specific Center for Cyber Excellence (COE) will make these collaborations easier to accomplish and more lasting, broadening the impact to bring about measurable improvements in the cyber-readiness of the workforce. At its administrative core, the COE is a streamlined central coordinating office to help build and maintain this state-wide collaborative construct to leverage all of the cyber-security partners under one cohesive organization. This “virtual” organization will enable each academic or industry partner to have the benefit of the best possible knowledge and access to expertise for their needs without having to support duplicative investment not germane to their goals.

The Oregon Center for Cyber Excellence (COE) will be a national asset to advance substantially the knowledge and educational strategies for cyber-education. The COE will build on results locally and contribute to the national dialogue in this area. The COE will establish a core capability in cyber-security education and research that deploys and integrates the intellectual capacity to deliver a cyber-savvy workforce for both industry and government. The COE will leverage existing consortiums, public-private partnerships, and government working groups to achieve its goals. But these structures alone will not provide the level of cohesion or continuity to the organization that this effort will require to be successful. Therefore there exists the ongoing need for a small cadre of dedicated staff to serve as the cohesive center of the COE. This COE Program Management Office (PMO) will manage the projects, exercises, and initiatives for starting up, operationalizing and documenting improvements to cyber-education and other cyber-readiness education goals. The PMO enables the academic and industry partners to function as a single, seamless yet flexible organization.

Central to the PMO oversight of performance against defined milestones, technology development and budget will be managed with a disciplined, business-oriented focus to ensure quality delivery of all elements of the COE mission. The approaches used in the COE PMO are designed to overcome the two primary obstacles of central support organizations: 1) the organizational strategies employed don't co-incentivize the organizations to collaborate; 2) the information sharing mechanisms were not particularly efficient.

The near term goal is to establish the COE Program Management Office, use the PMO to coordinate and execute an initial set of improvements, and build linkages with appropriate partners to establish the cyber-education community across the state. We believe this initial effort and the resulting lessons learned will enable the COE to quickly grow to serve the increasingly complex needs of the employers across the state.

SCOPE

The COE Implementation plan has three major objectives:

- Establish a Program Management Office function sufficient to support near term activities;
- Develop, coordinate, and execute outcome driven programs designed to ensure the long-term success of assigned initiatives; and
- Support the creation of a cyber-education community sufficient to meet the increasing needs of the industry for a larger and more skilled cyber-savvy workforce within the region.

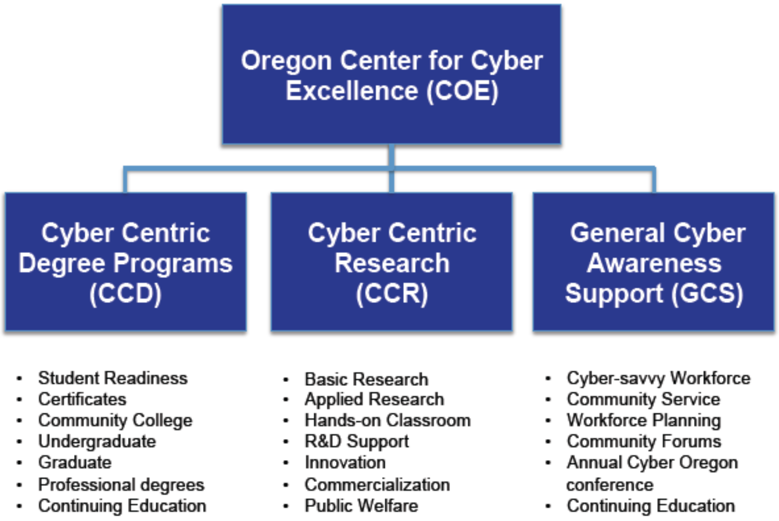


Figure 2: Proposed COE Program Structure

IMPLEMENTATION TASKS

Task 1 - Establish the COE Program Management Office

In order to best meet the near term and long term needs of the organization and the state the PMO will be organized into functional teams focused on the critical coordination and production needs. Three primary teams are envisioned: a Cyber-Centric Degree team, a Cyber-Centric Research team, and a General Cyber-Awareness Support team. This structure will allow for dedicated staff to focus on each of the partner constituencies and add value in achieving the COE objectives.

The Cyber-Centric Degree (CCD) Team will be focused on using both best practices and innovative new techniques to create more effective cyber-education programs. The CCD team will work with the other COE teams and the partners to establish and maintain a database or Oregon cyber education related curricula, initiatives, research and opportunities. The team will leverage the partners' existing databases and known activities but will also actively synthesize new cross-cutting opportunities to increase both the available population of cyber-students but also (importantly) the diversity of those students. We believe this approach will enhance and strengthen the results of all of the cyber-education done in Oregon. This team will be staffed by professional educators skilled in curriculum development and will leverage Oregon's existing student population by employing interns interested in the fields of education, psychology, human development and cyber-research.

The Cyber-Centric Research (CCR) team is tasked with ensuring the cyber-research in Oregon Universities is supporting both the needs of industry as well as the creating opportunities to train the next generation of cyber-experts. The team will facilitate the initial coordination of the industry partners to include the setting of information, data systems, and operational standards to ensure research conducted in the lab can be easily applied to real-world environments. They will work with each of the University partners initially and on an ongoing basis to help build programs to meet the established standards. At the direction of the industry partners they will seek out interested Oregon researchers to help with specific research needs. They would also assist in having university researchers validate solutions to emerging threats and demonstrate best practices to industry partners as needed. The CCR team would also be chartered to assist in pulling together research experts needed for incident response team needs across the state. This team will include professional staff familiar with a broad swath of cyber-research and industry needs.

The General Cyber-Awareness Support (GCS) team provides the most up to date information and access to cyber-resources across the education spectrum. This team provides a centralized resource for industry and government organizations to leverage as needed when questions on cyber-security arise. The GCS team will be responsible for organizing and executing the quarterly "best-practices" meetings as well as annual state-wide conferences on cyber-security education and training. The GCS team in conjunction with the CCR team will be responsible for organizing hands-on cyber-security competitions to promote active demonstration of cyber-expertise and critical thinking skills across all levels of students. The GCS team will include educators as well as program coordinators with skills in event planning, digital media outreach, and stakeholder engagement. They will produce stakeholder reports on the measured progress of the COE compared to the approved plan.

The three teams will work seamlessly to ensure the needs of the partners and other Oregon stakeholders are well met.

Task 2 - Facilitate and Support the Execution of Cyber-education Initiatives

In conjunction with Industry and other senior Oregon officials, the PMO will help build the cross-functional teams needed to address the challenges identified in the ETIC Cyber-Needs Assessment. The Program Manager will be responsible for project timeline management and tracking, financial management, information technology infrastructure, contracting and legal issues, public affairs, data compliance, technology venturing, and new funding development and administer and facilitate all necessary meetings and reviews required by the effort. The Program Manager and the PMO teams will ensure compliance with all applicable regulations and interface directly with the internal Oregon University System (OUS)[xliv] leadership, the General Counsel, and other offices as needed. Intellectual portfolio management and technology venturing will be accomplished effectively through the existing OUS mechanisms with intensive partnering with the respective technology transfer offices at partnering organizations.

Task 3 – Facilitate the Establishment of the Longer-term Changes Needed.

The major operational components of the proposed effort consist of the Oregon elected officials, the individual Industry and Educational partners', external advisors, as well as the Program Management Office. For this task the PMO staff led by the Program Manager will facilitate meetings with stakeholders and partner organizations to draft, modify, and obtain approval for the initiatives necessary to accomplish the mission of the COE. Under this task the PMO will also seek the input of external experts to assist with the formulation and evaluation of initiatives and outcomes. It is planned that the stakeholders will identify and independent panel to review the overall program bi-annually and provide a comprehensive critique to OUS regarding project progress and relevant recommendations to improve the program.

Task 4 – Document Lessons Learned and Progress to Date

The teams will incorporate lessons learned in tasks above into a final report, to include the combined, self-assessed capabilities of the research partners; any identified risk factors; lessons learned in the process of establishing the organization; and recommended actions for further growth.

COE IMPLEMENTATION SCHEDULE

TASK	First 6 months	Months 7-12	Months 13-18
Task 1 – Establish PMO	Staff in place; office operational	Begin internship program	Refine procedures
Task 2 – Facilitate & support cyber-education initiatives	Identify Initiatives, teams & resources. Assess need for Cyber-SRC.	Begin seminars and cyber-competitions.	Host first annual statewide conference
Task 3 - Longer-term Changes	Solicit more detailed feedback from stakeholders	Compile results, document initiatives, build support	Expand communication to reach more stakeholders
Task 4 - Lessons Learned	Report progress to plan	Collect feedback. independent assessment	Annual Progress Report

APPROACH

The implementation team will employ a four-part strategy to accomplish the objectives detailed in the paragraphs above. The PMO will implement a management structure designed to facilitate and catalyze technical and management success of the partners and stakeholders. The operational plan incorporates the following principal design elements:

- Commitment to development and delivery of innovative, high-value solutions appropriate to Oregon needs.
    - A responsive and closely coordinated interface with the stakeholders, including essential metrics
    - Strong, active participation of industry and academic partners, including an effective communication strategy
    - A results-focused operating and curriculum development plan
- Long-term strategic vision coupled with effective, practical decision making and stringent fiscal oversight including:
    - A transparent, team-based, cross-functional interdisciplinary construct
    - Sophisticated program management
    - Continuous feedback from external advisors

Part two of this strategy builds upon our understanding by articulating the types of risks the organization is likely to encounter and delineating the kinds of quality standards necessary to ensure the collective partner units function as a cohesive whole. Collaborative performance monitoring is a key attribute of an effective management system and will be critical for improving future planning, minimizing missed opportunities and fostering a culture of continuous improvement within the community.

Given these efforts, the third part of our strategy will be to work with our partner organizations to identify the best combined team for each engagement - be that a new course to be designed, a new type of incident response tool, a social media cyber-awareness campaign. This will include non-traditional approaches to team building, resource sharing, and program execution.

Part four of our strategy will seek to determine if there are any undiscovered vulnerabilities in our best-practices framework. Here we will ask colleagues and peers to scrutinize our practices, both to analyze our findings and to ensure that we have not overlooked any significant areas of opportunity to improve cyber-education practices and operations.

If approved, these activities can foster and perhaps facilitate the creation of a global network of professionals interested in improving clinical trial practices within the larger bio-research and development community.

RESOURCES

Approximately $3.0 million in initial funding will be needed to meet the needs of the tasks defined above. This includes full stand-up and staffing of the Program Management Office and provisioning the initial resources until the next budget cycle. Approximately $2.3 million per year is needed in the budget to sustain the program. The bulk of these funds are for personnel to set in place the collaborative initiatives needed to create a Center for Cyber Excellence in Oregon. Included in this cost is approximately $150k to establish the office including furniture, modifications to the space, office equipment and IT infrastructure.

Budget Category	Initial Phase (18 Months) $k	Ongoing Annual Operation $k
Labor	$ 2,475	$ 1,989
Travel	$ 18	$ 12
Equipment	$ 62	$ 0
Materials & Supplies	$ 23	$ 15
Other Direct Costs	$ 397	$ 243
Total	$ 2,975	$ 2,259

Table E-1. Estimated PMO expenses. Comparison of stand-up (first 18 months) versus annual expected run rate for ongoing operations with a full staff.

There is suitable, existing office space in OUS and other Oregon State government facilities. The COE should be centrally located to best access to both industry and academic centers.

The total cost for the defined effort will be $3.0 million with over 80% budgeted for Direct Labor, 12-15% for Other Direct Costs (includes $150k for establishing the office environment), and small percentages for the other categories. Travel is budgeted to cover the travel costs of the PMO team to visit key facilities around the state, recruit participants, and meet with partner leadership. Other Direct Costs include funds for the support of the conferences and competitions as well as funds for external evaluation and production of reports. For a more detailed breakdown see the Basis of Estimate to follow.

Basis of Estimate Detail

Please note this budget justification is focused on the tasks for this effort and does not reflect projected research programs or other into costs.

Personnel (Labor):

- Program Manager: Significant Contributor at the Executive Director level, 100% effort for 18 months at $140,000 per annum base salary; The Program Manager provides the overall project leadership and coordination.

- Team Managers (3): CRM/Program Manager categories; 100% effort @ $130,000 p.a. for 16 calendar months during start-up; The Team Managers lead their respective areas with minimal direct supervision, coordinate with the Program Manager to facilitate the running of the program, and ensure the achievement of goals, benchmarks and fiscal management for their area.

- Research Analysts (2): 100% effort for 16 calendar months at start-up, 2 @ $75,000 p.a; the analyst's primary responsibility will be assisting with targeted volunteer recruitment and enrollment support.

- Program Coordinators (3): 100% effort for 16 calendar months at start-up, 3 @ $60,000 p.a; the program coordinators main function will be to assist the Team Managers and the Program

Manager with the programmatic, scientific, fiscal management and information dissemination for the project.

- Administrative Assistant: 100% effort, 18 calendar months at start-up, $50,000 p.a; the administrative assistant will facilitate all administrative responsibilities of the project including, but not limited to, planning meetings, travel, preparation of reports and manuscripts, and other general administrative duties.
- Student (5): 100% effort, 12 calendar months at start-up, 10 @ $13,200 p.a.; each Student will be assigned specific tasks by the Team Managers and the Program Manager consistent both with their studies and with the programmatic, scientific, and other goals of the project.
- Graduate Research Assistant (3): 100% effort, 12 calendar months at start-up, 5 @ $66,000 p.a; each GRA will be assigned specific tasks by the Team Managers and the Program Manager consistent both with their studies and with the programmatic, scientific, and other goals of the project.
- Payroll and benefits: estimated at 45% of base payroll costs.

Travel: Funds are requested for local travel (mileage) based upon federal mileage reimbursement rates and projected local coordinated meetings for 18 months @~$500/month. Funds are also requested for out-of-town (overnight) meetings with projected expenditures being for four individuals to travel annually with each person trip @ $1,500.

Equipment: Funds are requested to cover initial expenses associated with regular office automation equipment including laptops, printers, and fax machines. It is expected to be a combination of new and used equipment. The budget equates to approximately $2,500 per person in the office. Total funds requested: $45,000.

Materials and Supplies: Funds are requested to cover expenses associated with running the office including general office supplies, postage, and other consumables. It equates to approximately $50 per person in the office per month. Total funds requested: $60,000.

Other Direct Costs:

- Services – The largest single estimated setup cost. A reserve of $100k will be set aside, pending finalization of office space. In recent times, new office spaces have required tenant renovations on the order of $100 - $400k to make the space work for the new function. This could also include the cost of new modular furniture (aka cubicles) if the space is already constructed with an open floor plan. Expected ongoing facilities costs are $100,000 p.a. Total Funds requested: $250,000 for start-up.
- Communications – the request is to cover the costs of office phones, IT support and data service for all staff. The estimate includes setup charges and service fees for the period of performance. Total Funds requested: $45,000.
- Miscellaneous – Includes other office costs and any Publication charges for conference or other promotional materials. Total funds requested: $7,500.
- Conference and Event Expenses - Bi-monthly topic specific update/outreach meetings to be held around the state will provide industry the latest research findings and best practices (6 @ $5,000 per year). The annual conference including both outreach and education will be partially supported by registration fees with discounts for students. Based on projected scope, the net investment for the annual conference costs is estimated at $40,000 per year. The cyber-competition will maximize the use of donations for software, equipment, and awards. The net investment for facilitating the cyber-competition is estimated to cost $25,000 per year to cover costs for facilities, equipment, and supplies. Total event funds requested: $95,000.

REFERENCES

[i] Tripwire, Compli, Galois, Smarsh, Simple, NTT Centerstance, Tonkon Torp, Davis Wright, Marger Johnson & McCollom, Perkins & Company, Portland Seed Fund, and Silicon Valley Bank

[ii] 2012 Internet Crime Report IC3.gov, FBI page 5 http://www.fbi.gov/news/stories/2013/may/internet-crime-in-2012/internet-crime-in-2012

[iii] 2012 Internet Crime Report IC3.gov, FBI page 5 http://www.fbi.gov/news/stories/2013/may/internet-crime-in-2012/internet-crime-in-2012

[iv] Privacy vs. Protection: A Delicate Balance, by Maryan Lawlor, AFCEA, November 2001: http://www.afcea.org/content/?q=node/482#sthash.z1s80h2y.dpufhttp://www.afcea.org/content/?q=node/482

[v] http://www.mdchhs.com/blog/cybermaryland-conference-privacy-versus-protection

[vi] http://proceedings.esri.com/library/userconf/proc96/TO200/PAP173/P173.HTM

[vii] http://www.huffingtonpost.com/marc-rotenberg/privacy-vs-security-priva_b_71806.html

[viii] Landwehr, C.; Boneh, D.; Mitchell, J.C.; Bellovin, S.M.; Landau, S.; Lesk, M.E., "Privacy and Cybersecurity: The Next 100 Years," Proceedings of the IEEE , vol.100, no.Special Centennial Issue, pp.1659,1673, May 13 2012: URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6182691&isnumber=6259910

[ix] Lack of cyber pros puts US in dangerous position, by Kevin Coleman, GCN, Jun 28, 2011, http://gcn.com/articles/2011/06/08/digital-conflict-cyber-worker-shortage.aspx

[x] “Cyber security industry launches skill search” , By Hannah Kuchler, Financial Times, 24 February 2014, http://www.ft.com/intl/cms/s/0/b7d0dce4-923e-11e3-8018-00144feab7de.html?siteedition=intl#axzz2xOGzLRfw

[xi] U.S. cyberwarfare force to grow significantly, defense secretary says, By Ellen Nakashima, Washington Post March 28, 2014, http://www.washingtonpost.com/world/national-security/us-cyberwarfare-force-to-grow-significantly-defense-secretary-says/2014/03/28/0a1fa074-b680-11e3-b84e-897d3d12b816_story.html?wpisrc=nl_eve

[xii] Understaffed and at Risk: Today’ s IT Security Department, Ponemon Institute , January 2014

[xiii] “Cyber security industry launches skill search” , By Hannah Kuchler, Financial Times, 24 February 2014, http://www.ft.com/intl/cms/s/0/b7d0dce4-923e-11e3-8018-00144feab7de.html?siteedition=intl#axzz2xOGzLRfw

[xiv] With $12M donation, Tripwire aims to educate next generation of cybersecurity experts, Portland Business Journal online Apr 10, 2014 http://www.bizjournals.com/portland/blog/2014/04/with-12m-donation-tripwire-aims-to-educate-next.html

[xv] http://online.wsj.com/news/articles/SB10001424052702303847804579481500497963552?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702303847804579481500497963552.html

[xvi]STEM Stinks For Cybersecurity by Richard Stiennon, Forbes (TECH) 23 March 2014 http://www.forbes.com/sites/richardstiennon/2014/03/23/stem-stinks-for-cybersecurity/print/

[xvii] Understaffed and at Risk: Today’ s IT Security Department, Ponemon Institute , January 2014

[xviii] Schneider, F. B. (2013). Cybersecurity Education in Universities. Security & Privacy, IEEE, 11, 3–4. doi:10.1109/MSP.2013.84

[xix] http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml

[xx] http://niccs.us-cert.gov/education/national-centers-academic-excellence-cae

[xxi] http://www.nsf.gov/news/news_summ.jsp?cntn_id=128679

[xxii]http://www.computerworld.com/s/article/9246532/IT_pros_rank_University_of_Texas_San_Antonio_best_school_for_cybersecurity

[xxiii] http://www.ponemon.org/library/archives/2014/02

[xxiv] GWU targets cyber security By Adam Palin FT 20 May 2013 http://www.ft.com/intl/cms/s/2/3112eb22-b344-11e2-b5a5-00144feabdc0.html#axzz2xOGzLRfw

[xxv] http://www.ponemon.org/library/archives/2014/02

[xxvi] http://nationalccdc.org/index.php/competition/about-ccdc/history

[xxvii] TAO recognizes the OUS will not continue, however, at the writing of this report, no determination was made regarding a replacement for leadership or stewardship. We look forward to working within the ultimate structure to successfully create a COE for Oregon.

[xxviii] http://www.dhs.gov/stopthinkconnect-cyber-awareness-coalition

[xxix] http://www.nsa.gov/academia/nat_cae_cyber_ops/index.shtml

[xxx] http://chronicle.com/article/Federal-Agencies-Revamp/141953/

[xxxi] http://www.cyberwatchwest.org/index.php?option=com_content&view=article&id=73&Itemid=127

[xxxii] http://www.nsa.gov/ia/academic_outreach/nat_cae/seal_program.shtml

[xxxiii]http://www.cerias.purdue.edu/site/blog/post/centers_of_academic_adequacy/

[xxxiv]http://www.cerias.purdue.edu/site/blog/post/centers_of_academic_adequacy/

[xxxv] http://www.nsf.gov/pubs/2014/nsf14510/nsf14510.htm?org=DGE#toc

[xxxvi] http://niccs.us-cert.gov/education/national-centers-academic-excellence-cae

[xxxvii] http://www.cyberwatchcenter.org/

[xxxviii] http://www.cyberwatchcenter.org/index.php?option=com_content&view=article&id=67&Itemid=166

[xxxix] http://www.cssia.org/index.cfm

[xl] http://www.cs.cmu.edu/overview-programs

[xli] http://business.utsa.edu/news/2014/cybersecurity_ranking.aspx

[xlii] http://www.washington.edu/research/centers/126

[xliii] https://ciac.ischool.uw.edu/

[xliv] We understand the structure of the OUS system may be undergoing change. It is important for the center to be managed by an organization with an impartial, statewide mission.