Healthcare & Public Health Sector Coordinating Council

PUBLIC PRIVATE PARTNERSHIP

Healthcare Industry Cybersecurity Workforce Guide

Recruiting and Retaining Skilled Cybersecurity Talent

The Health Sector Coordinating Council and the Cyber Workforce Development Initiative

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-sector critical healthcare infrastructure entities organized under Presidential Policy Directive 21 and the National Infrastructure Protection Plan to partner with government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public. The HSCC Joint Cybersecurity Working Group (JCWG) is a standing working group of the HSCC, composed of more than 220 industry and government organizations and 27 advisors working together to develop strategies to address emerging and ongoing cybersecurity challenges to the health sector.

Recognizing the increasing cybersecurity threats to the healthcare sector, the Congress passed the Cybersecurity Act of 2015 which, among other things mandated that the U.S. Department of Health and Human Services establish a task force of industry and government experts to assess gaps in the cybersecurity of the healthcare system and propose recommendations for addressing those gaps. Among the six major imperatives recommended by the Healthcare Industry Cybersecurity (HCIC) Task Force in June 2017 was Imperative 3 – "Develop the healthcare workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities."

The HCIC workforce-oriented recommendations include: 1) Identifying the cybersecurity leadership role for driving robust policies, processes and functions with clear engagement from executives; 2) Establishing a model for resourcing the cybersecurity workforce with qualified individuals; 3) Creating Managed Security Service Provider models to support small and medium-sized healthcare providers; and 4) Evaluating options for small and medium-sized providers to migrate patient records and legacy systems to secure environments.

The HSCC Joint Cybersecurity Working Group (JCWG) in turn established a number of task groups to address the many HCIC recommendations, including a task group on Workforce Development.

The HSCC JCWG assigned the Workforce Development Task Group (WDTG) to assess the risk to critical healthcare infrastructure as a result of issues with recruiting, training, and retaining cybersecurity professionals, and to offer the industry basic and useful tactics for building a pipeline of qualified employees and cybersecurity management along the spectrum of skills and responsibilities.

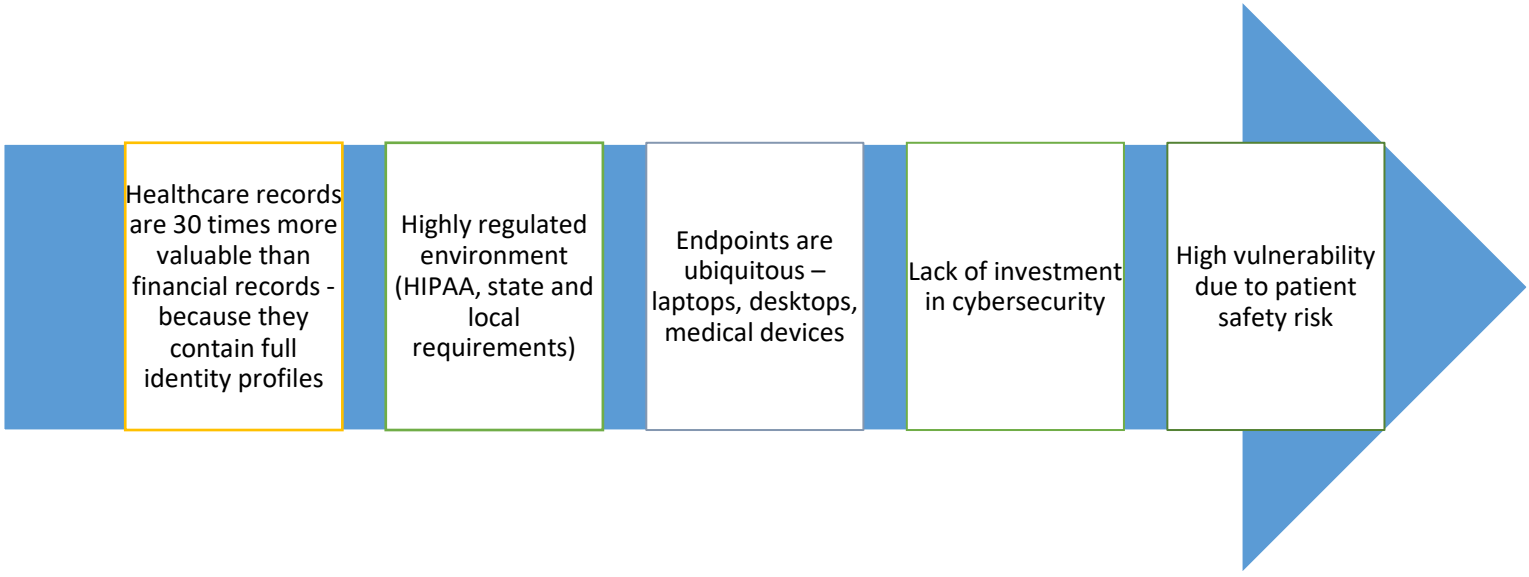
In considering useful parameters for this assessment, the WDTG observed that there are two "buckets" for cybersecurity education and training in the healthcare sector. The first is the cybersecurity training necessary for a healthcare professional to do their job. This falls into the category of "cybersecurity awareness" of business-side employees to take necessary administrative (non-technical) steps to protect personal identity information (PII) or protected health information (PHI), or avoid missteps such as falling for social engineering threats or practicing unsafe online activities on enterprise networks or applications. This training is not technical and there is no presumption that the recipients' jobs are technical in nature. This falls under the "Cybersecurity is Everyone's Job" guidebook, which is a work product of the NICE working group subgroup.

The other bucket involves technical personnel whose roles involve the management of data, information technology, network and application security, and some of the newer blended information and device management roles in the healthcare field.

It is this technical segment of the healthcare workforce that this resource is intended to address - to help healthcare organizations, particularly those with tight budgets and lacking onboard cybersecurity expertise, adopt impactful methods and programs for recruiting, retaining and training more skilled and available cybersecurity human resources.

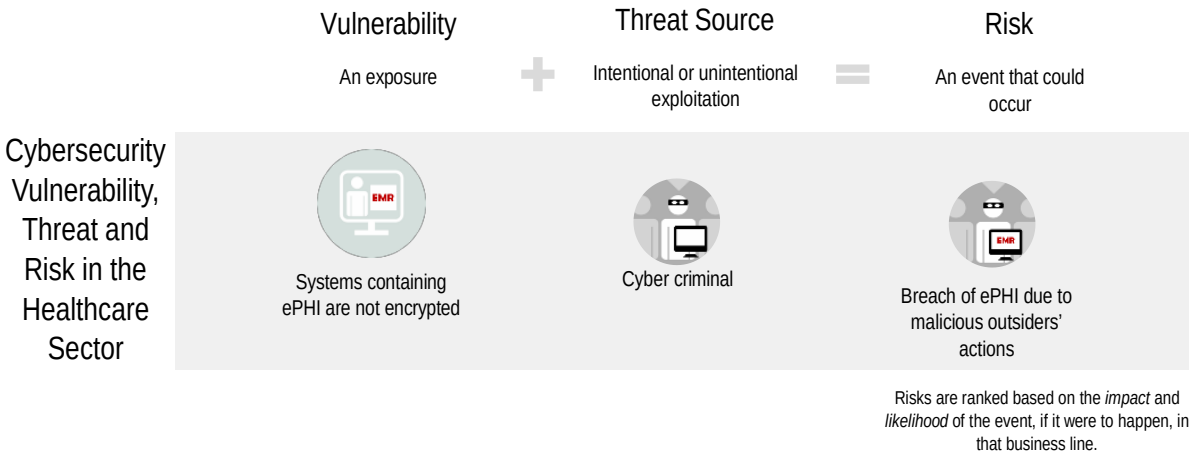
The Cybersecurity Workforce Challenge

The HSCC's mission in all aspects of cybersecurity is grounded in the recognition that patient safety increasingly depends in no small measure on cyber safety. In turn, cybersecurity depends on a knowledgeable workforce of both technical experts who manage enterprise security, and the front-line clinicians whose constant touch of both technology and patients is the last line of defense. Cybersecurity is thus a shared responsibility. It is not just a technical job, but one that reaches across enterprise business and operational roles, and up to the C-Suite. This imperative stems from the perforation of enterprise boundaries, with clinical use of mobile devices, employee remote access, connected medical devices and "Internet of Medical Things", and outsourced software-as-a-service.



Why is a Robust Cybersecurity Workforce Needed in Healthcare?

Our risks and our responsibilities are shared. As such, we must reduce risk across the ecosystem if we are to contribute to a workforce culture of security that manages cyber risk toward a more secure and resilient healthcare system. This culture ultimately supports patient health and safety. It is by advancing this proposition to our cybersecurity professionals – that they are not just technical overhead, but part of the *public good* of public health and safety – that we can attract the best talent that works in partnership with health practitioners in a clinical environment that understands and invests in the linkage between cyber safety and patient safety.



This imperative for implementing appropriate cybersecurity practices in a clinical environment is embodied in another resource developed and published December 28, 2018 under the auspices of the HSCC: the "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients." This resource offers several real-world threat scenarios that illustrate how cyber professionals must work with health practitioners to ensure patient safety through a range of technical controls and user/health provider due diligence:

- **Email Phishing Attack:** Your employees receive a fraudulent e-mail from a cyber-attacker disguised as an IT support person from your patient billing company. The e-mail instructs your employees to click on a link to change their billing software passwords. An employee who clicks the link is directed to a fake login page, which collects that employee's login credentials and transmits this information to the attackers. The attacker then uses the employee's login credentials to access your organization's financial and patient data.
  Impact: A pediatrician learns that an attacker conducted a phishing attack to steal their patients' data and commit an identity theft crime.

- **Ransomware:** Through an e-mail that appears to have originated from a credit card company, a user is directed to a fake website and tricked into downloading a security update. The so-called

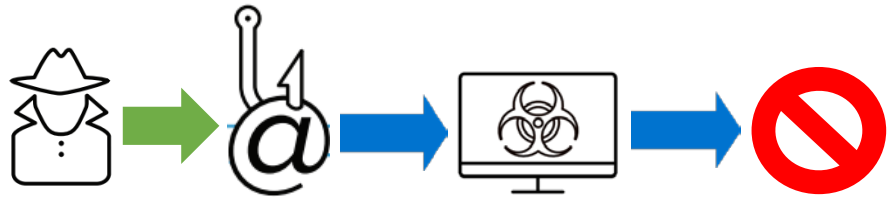
security update is actually a malicious program designed to find and encrypt data, rendering them inaccessible. The program then instructs the user to pay a ransom to unlock or unencrypt the data.
Impact: A practitioner cannot view patient charts because of a ransomware attack that has made the electronic health record (EHR) system inaccessible.

- **Loss or Theft of Data and/or Equipment:** A physician stops at a coffee shop and uses its public Wi-Fi to review radiology reports. A nearby thief scanning for vulnerable devices hacks the laptop without the physician's awareness and steals a trove of patient data.
  Impact: Loss of sensitive data because of the use of high-risk public Wi-Fi may lead to a clear case of patient identity theft, and, with thousands of records potentially stolen, the physician's reputation could be at stake if all the patient records make it to the dark web for sale.

- **Insider, Accidental or Intentional Data Loss**: An attacker impersonating a staff member of a physical therapy center contacts a hospital employee and asks to verify patient data. The imposter then is able to acquire the entire patient health record.
  Impact: The patient's protected health information (PHI) was compromised and used in an identity theft case. The patient attributes the data loss with the last visit they had at the health system and associated providers.

- **Attacks Against Connected Medical Devices**: A cyber attacker gains access to a care provider's computer network through an e-mail phishing attack. While scanning the network for devices, the attacker takes control of a file server, allowing access and control (e.g., power off, continuously reboot) of all the heart monitors in the ICU, putting multiple patients at risk.
  Impact: Patients are at great risk because an attack has shut down heart monitors, potentially during surgery and other procedures. Nurses and physicians required to staff the unit in a downtime state may not be available for a period of hours

- **Third party risks:** A supplier of medical coding services inadvertently exposes a database server to the public internet. The error is not found until a patient does an internet search on their name and sees their latest hospital visit documented on web page.
  Impact: The risk of a cyber-event originating from a vendor or supplier that uses PHI on behalf of the provider organization may lead to patient identity theft, including attempts at fraudulent medical care, and loss of faith in the physician or health system.



External threat agent distributes malicious file attachment or link through email spam.

User clicks on the attachment or link and infects the user's computer or shared drives with ransomware.

Disrupts operational business and patient care, with financial impact

Taking the above graphic into consideration, to adequately prepare for and mitigate the cyber threats, health providers must appoint and empower cybersecurity leadership to design and enforce an

enterprise-wide strategy to protect patient lives, hospital data and operations, and cultivate a culture of cybersecurity as a shared responsibility. Provider management should also ensure that cybersecurity professionals are trained to an appreciable understanding of the clinical environment in which healthcare providers operate. Clinicians likewise must understand the importance of the cyber professional's job in helping them protect hospital operations and patients from the effects of cyber attacks.

Finding and retaining qualified cybersecurity staff for the health provider enterprise, however, is a significant challenge because of the competition for insufficient numbers of talented professionals and inadequate cybersecurity budgets. This is a strain not just within the health sector, but across business and government. According to the International Information System Security Certification Consortium, or (ISC)², there will be 1.8 million unfilled cybersecurity jobs in the U.S. by 2022. A recent 2018 HIMSS Cybersecurity Survey found that 75% of surveyed organizations experienced a significant cyber event in the previous 12 months, while barely more than 50% have allocated cybersecurity budgets. About the same percentage identify lack of qualified personnel as the biggest barrier to remediating cyber incidents.

It is clear that health organizations must be creative and flexible in finding the appropriate leadership and staff, with appropriate skills, at the right price. This paper will address several ideas. There are no silver bullets, but a committed organization can improve their capabilities in managing cybersecurity risk.

NICE Cybersecurity Workforce Framework

For a more comprehensive programmatic approach to workforce development, hiring and training, please refer to the various tools and resources that have been developed in a public private partnership led by one of the key HSCC partners in this field – the National Institute of Standards and Technology's National Initiative for Cybersecurity Education (NICE). The NICE "Cybersecurity Workforce Framework" improves communication about how to identify, recruit, develop, and retain cybersecurity talent. It is a resource from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of workforce development, planning, training, and education. The Framework serves as a fundamental reference to support a workforce capable of meeting an organization's cybersecurity needs. It provides organizations with a common, consistent lexicon that categorizes and describes cybersecurity work by Category, Specialty Area, and Work Role. It provides a superset of cybersecurity Knowledge, Skills, and Abilities (KSAs) and Tasks for each work role. The NICE Framework supports consistent organizational and sector communication for cybersecurity education, training, and workforce development, both within the enterprise and those Business Associate vendors and service providers in the healthcare ecosystem.

The NICE Framework is based in part on notion that even without healthcare specific roles, anyone whose position involves handling of patient information or management of outsourced services, should be evaluated against the framework. Their tasks should be defined and made part of their job description. This activity involves individual contributors, managers, human resources, employee stakeholder groups such as union staff for buy-in, etc. Roles requiring some cybersecurity workforce categorization will touch entire organization (legal, policy, governance, strategy, as well as the expected patient-facing roles.) Even a small healthcare provider that outsources their IT and cybersecurity will have a person(s) who discusses the various guidelines, directives and requirements they must adhere/meet.

Building the Cybersecurity Workforce Ladder and Management Criteria

This resource categorizes and frames key rungs of the cyber workforce ladder, from the first step of: 1) Hiring students, to 2) Transitioning IT staff to cybersecurity responsibilities; 3) Developing and managing professional development programs for executive-track cybersecurity personnel; and 4) Outsourcing critical functions not otherwise resourced within the enterprise.

Human Resources and executive management within a health delivery organization or other healthcare company should look to these examples as starting points for brainstorming your organization's contributions, not just to your enterprise security staff but to the healthcare ecosystem as a whole.

I. Student Staffing Pipeline

Goal: Students develop cybersecurity skills with part-time work, internship, or externship work while attending school. The goal doesn't stop at hiring students. The organization must turn them into effective members of the cybersecurity mission, allowing them to perform work in a way that they are not viewed simply as "students" by the organization—but viewed as cybersecurity professionals.

Myth: Students become a "babysitting job" for already busy staff, entry-level people won't help the situation.

Truth: Several organizations that have committed to student programs have learned and can testify that a large percentage of students show up with cybersecurity skills they can use immediately. They learn to manage a handful of processes or tools within days to a few weeks.

Further, many of these organizations learn that such additions to the cybersecurity team add a new dynamic, motivating existing full-time staff performance.

Additionally, existing cybersecurity managers and staff are often willing to share their expertise and knowledge to assist in the technical and professional development of these new staff resources.

Tactics for Success:

Contact nearby higher education institutions. Reach out to community colleges, universities (undergraduate and graduate level), etc., about existing programs for placing students into the local workforce. Many higher education institutions are using grant funding to work with businesses on student staffing and internship opportunities. Labor costs range from just providing the internship opportunity, to around $12-$18 per hour for continuous part-time student staff.

Leverage university credit hours as internship compensation for students. Students need a certain number of credits to fulfill graduation requirements. Offering credit hours in exchange for cybersecurity-related work is a step in addressing the current cybersecurity workforce shortage–in the labor market and within an organization–and puts a student closer to graduation. As academic-credit programs for internships vary by institution, it is important to coordinate ahead of time with your local colleges and universities about appropriate credits to be offered as part of the recruitment process.

Have a plan. Have you identified existing functions that could benefit from additional resources? Or are there new processes or tasks that a new resource can help to establish and formalize? Which event or incident flows happen frequently enough to document and teach someone to take over? Which SLAs are being missed, or just not established, because there isn't a dedicated resource to manage them? What "checklist items" must be done every day/week/month for compliance, assurance, etc.?

Learn to evaluate students. Undergraduates who are fresh out of school, veterans returning to school, and grad-students may present different skillsets based on their prior experience. Some may have a skillset related to business operations, risk, and regulatory dynamics, while others might have an affinity for programming, website development, ethical hacking or other STEM areas. It is important for the hiring organization to learn these distinctions and use them to its advantage.

Balance expectations. Expectations and responsibilities for interns should be in alignment with and supplement the intern's primary role as "student." For many of these interns, especially those in rigorous programs, their classwork will take priority over their internship, even while their skills may encourage managers to give them increased responsibilities that can create new areas of risk if they become unavailable for a period of time due to course load.

Here are examples of student staffing resources leveraged by Sentara Healthcare in Virginia:

http://csiip.spacegrant.org/VCAI

https://www.cyberva.virginia.gov/

Criteria for Success:

Students being hired into full-time cybersecurity jobs after graduation. The full-time job may be with the healthcare organization they started with, or with another healthcare organization. A qualified “success” is a student joining the healthcare cybersecurity workforce—somewhere. If your organization is able to train college students to the point that they become viable cybersecurity candidates at other health organizations, you’re doing it right! If members of your organization interact with your students and don’t realize they are students, you’re doing it right. If you miss them while they are at school, you’re doing it right.

Failure Example: Students leave the opportunity at your organization to work at a lower paying job that does not apply the cybersecurity knowledge and expertise they gained.

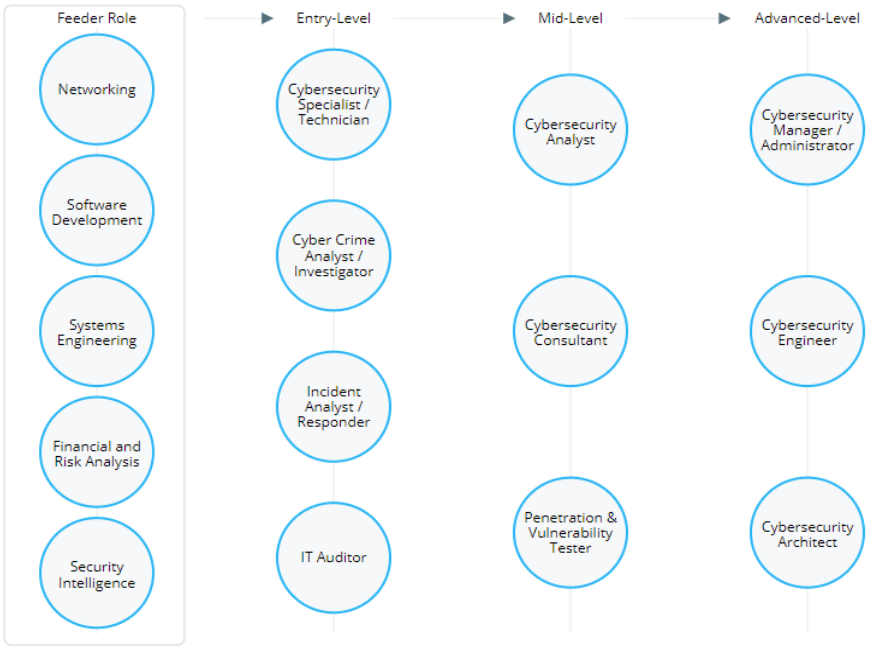
However, externship opportunities may also be leveraged (typically, a shorter experience and without compensation). The possibility of getting credit(s) for such externships may be explored with the institutions of higher learning.

II. IT Staff Conversion to Cybersecurity

Goal: Develop a plan of success and cybersecurity awareness for IT professionals or clinical engineers to make the transition from traditional IT roles to cybersecurity roles, including mentoring, educational support, and outreach.

Tactics for Success:

Cybersecurity Career Pathway Fields*



* https://www.cyberseek.org/pathway.html

Address the basics. Training and preparation to pursue the Certified Information Systems Security Professional (CISSP) certification offered through local or regional groups such as Information Systems Security Association (ISSA) is very affordable. The Health Care Information Security and Privacy Practitioner (HCISPP) certification is also a good option, with specific healthcare focus. Getting IT-to-cybersecurity converts acclimated to the world of cybersecurity through these programs allows them to compare what is happening at work with the total discipline set of a well-rounded cybersecurity program.

Other related certifications include Certified Healthcare Privacy and Security administered by the American Health Information Management Association (AHIMA) and the Associate Healthcare Provider Continuity Professional and the Certified Healthcare Provider Continuity Professional (CHPCP).

Vet those who are sincerely interested in taking on completely new challenges and willing and interested to work in the cybersecurity field and its composite functions that continually evolve.

Develop an internal cybersecurity career roadmap within the organization for employees interested in the cybersecurity field. Consider opening the doors to the cyber field for non-cybersecurity professionals who show sufficient competency within their respective healthcare organization. This may require the involvement of human resources in mapping out the path for a successful transition. An initiative of this kind has the potential to cut down on employee turnover and incentivize retention.

Recruit and Mentor. Mentoring and outreach should be inclusive of all capable and interested professionals. Consider developing an internal security internship program to help current employees better understand the opportunities as well as help current managers vet the aptitude of these candidates.

Individuals in a variety of roles in IT are potentially good candidates to transition to cybersecurity roles. These include IT Operations, IT Architecture/Engineering, Application Development, Change

Management/Process Improvement, etc. Depending on their experience and areas of expertise, these individuals would probably be a better fit to transition to certain cybersecurity domains.

Developing basic cybersecurity awareness around the existing IT staff. Structured and repeatable processes for patch management, access controls and change management can have a profound impact on an organization's cybersecurity resilience. Small organizations that lack a fulltime cybersecurity team may need to develop cybersecurity awareness training programs for existing IT staff. Throughout the public and private sectors there are training services that organizations can take advantage of to properly train staff on cybersecurity.

Current entry level position descriptions may challenge new cybersecurity hires. Employers may need to take a risk on competent entry level cybersecurity candidates even if they fall short on specific knowledge, skills and abilities (KSAs). Potentially successful applicants with a learning driven mindset could fall through the cracks during resume review by human resources if they are not seen as having the "right" qualifications. Consider opening cybersecurity positions to candidates who may fall short of requirement expectations (certification, years of prior experience, etc.) but show clear potential for on-the-job skills acquisition and leadership development. This can potentially reduce new-hire costs, increase new employee loyalty, and develop longer term value-add to healthcare cybersecurity within the organizations and the sector.

Criteria for Success: Converted professionals remain in the cybersecurity field and become skilled enough to qualify for cybersecurity jobs at other organizations.

Failure Example: Professionals go back to old IT jobs, or develop only enough cybersecurity awareness and abilities to be valuable in their current, non-cyber position.

III. Cybersecurity Staff Professional Development and Retention

Goal: Enhance skillset of existing cybersecurity staff to augment program capabilities. Enable greater individual professional growth and support with education, mentoring programs, and outreach.

Tactics for Success:

Ongoing leadership or skillset development and educational or training experiences. For example, training on HIPAA security program management, ethical hacking, vulnerability management, penetration testing, etc.

Team exchanges with peers in other organizations, especially other healthcare organizations. For example, send your security operations center (SOC) manager to shadow a peer at another health system; send your deputy chief information security officer (CISO) to shadow a CISO at another organization; encourage and plan staff-level collaboration with peers at other organizations.

Exchange information on certification programs, workshops, webinars, conferences, etc.

Provide information on resources for peer-to-peer information sharing, mentoring, and support. This may include public and/or private peer information sharing groups within which practices, including both successes and failures, can be shared amongst peers.

Criteria for Success: Professionals at all levels of the team feel validated that the organization's cybersecurity program is benchmarked with appropriate peers, and that individual skillsets are aligned with those of their peers.

Having an opportunity for candid discussions with peers at other systems provides validation about alignment of resources, assignment of priorities, and validation of which vulnerabilities are common among other systems.

Providing insight to executive leadership that your cybersecurity organization and team have compared measures with appropriate peers on people, process and technology helps build more powerful business cases, and drives more candid discussions about risk tolerance.

Failure Examples: Team not equipped to deal with contemporary threats and vulnerabilities. Individuals dissatisfied from being locked into the same job. Cybersecurity program leadership not able to articulate how well their program aligns with current industry best practices.

New threats and vulnerabilities are discovered frequently. Failing to keep cybersecurity staff updated on new threats and vulnerabilities puts your organization at risk.

Many options don't need to cost a lot of money. Making sure all the appropriate people on your team have access to protected information sharing "Amber Lists" of vetted members of the Health Information Sharing and Analysis Center (H-ISAC); subscribe to information bulletins from the U.S. Computer Emergency Response Team (U.S-CERT); and are collaborating often with peers and vendors can keep them "updated" on what is happening. And even though many of these resources are inexpensive or freely available, consideration should be given to how these resources will be consumed, and what actions will be taken in response to "critical" alerts.

As team members develop, leadership should start mapping skills to their cybersecurity roadmap. Are there advanced skill needs in programs such as forensics, Governance Risk and Compliance (GRC), software development security operations (DevSecOps), penetration testing, etc. Leadership must be looking ahead at developing the right people and budgeting for advanced, or specific training needs.

IV. Outsourcing Select Cybersecurity Functions or Capabilities

Goal: Compensate for deficiencies regarding specific skillsets and/or need for 24x7 staffing. Not all organizations have reached a point of maturity for a fully functional and staffed organization. Some locations may have difficulty recruiting and retaining particular disciplines.

For example, finding experts in the GRC discipline, the ability to fully staff a 24x7 SOC, or a full-time need for penetration testers, presents challenges for some organizations in terms of recruiting and/or retaining the right people they can also afford.

Tactics for Success:

Do a skill-set review of cybersecurity staff and determine where there are gaps in skill-sets relative to the organization's cybersecurity road map.

Do a review of cybersecurity staff and working shifts and determine where gaps exist in terms of time (e.g., late night, holidays, emergency on-call, etc.).

Establish and document a business case addressing risks and include a cost benefit analysis.

Carefully select and vet service providers based on capabilities, scalability, cost and other set criteria.

Define metrics for success regarding "outsourced" cybersecurity staff performance. In addition to traditional operational metrics, an outsourced cybersecurity arrangement, such as "managed security services (MSS)" and "managed detection and response", will include service level agreement (SLA) measures. Some examples:

- Percent of security devices monitored (are you getting everything you paid for?)
- Customer comparisons (events received, incidents, top 5 attacks, etc.) to maximize and normalize the value of the managed service
- Customer satisfaction: often neglected but the best managed security services are an extension of the internal team.
- The mean time it takes between alert and remediation (including events remediated by internal teams).
- Number of indicators of compromise (IoC's) found in the environment, weekly. If the number is high, more than one or two per week, it could indicate the MSS is slow or does not have sufficient threat intelligence.

There are many more SLA types of measures that are important in an outsourced arrangement. In the end, the organization can delegate the performance of security services, but not the responsibility of information protection. Proactive review of the MSS arrangements is key.

Criteria for Success: The service provider is managed and viewed as part of the cybersecurity program, not viewed as a discrete function to manage.

Service providers are included in leadership's cybersecurity strategy and roadmap planning as appropriate.

Cybersecurity leadership fully understands roles and responsibilities for each side of the relationship. For example, many cybersecurity leaders assume it is the Managed Security Services Provider (MSSP) SOC's job to be sure log events are flowing from the organization's system to the MSSP's security information and event management (SIEM) tool. This is seldom written into a contract by default. The enterprise needs to outline clearly how the outsourced provider and/or specific outsourced services will be managed and governed.

A Health Sector Coordinating Council Cybersecurity Working Group white paper is scheduled for publication in Q3 2019 that will provide relevant guidance on establishing an enterprise-level third party supply chain risk management structure.

Failure Examples: Continuous dissatisfaction, failure to resolve problems or escalate issues, lack of competent outsourced staff, failure in timely communication, etc.

V. Non-traditional sources of workforce

With every credible source claiming there are millions of unfilled cybersecurity positions either now or in the very near future, healthcare organizations are going to have to seek solutions in non-traditional areas. In this document, there are examples given for sources like students, outsourced vendors, and non-IT

healthcare workers. To expand the options, non-traditional sources are worth discussing. Public-private efforts should be focused on developing these ideas and additional initiatives.

Neurodiversity Programs. Autism Spectrum Disorder includes a range of conditions characterized by challenges with social interactions, speech, repetitive behaviors, and non-verbal communication. Individuals with autism also have unique strengths and differences in specific areas where they may excel in a given discipline, such as cybersecurity roles.

For example, two organizations - Microsoft and Ernst and Young LLP (EY) - have successfully increased diversity in their cybersecurity workforce by hiring individuals on the autism spectrum. In 2016, EY launched a neurodiversity program to employ individuals on the autism spectrum into a variety of roles. It now employs 60 individuals on the spectrum in its advanced centers of excellence in Dallas, Philadelphia, Chicago and San Jose as part of its team of cybersecurity, artificial intelligence (A.I.) and managed services analysts. Healthcare organizations can model these efforts to attract talent and build an inclusive approach to developing a cybersecurity workforce that allows those on the autism spectrum to contribute in a meaningful way.

Microsoft's Autism Hiring Program : https://www.microsoft.com/en-us/diversity/inside-microsoft/cross-disability/hiring.aspx#coreui-heading-sp7tqqo

Ernst and Young Neurodiversity Program: https://www.ey.com/Publication/vwLUAssets/EY-neurodiversity-driving-innovation-from-unexpected-places-may-2018/$FILE/EY-neurodiversity-driving-innovation-from-unexpected-places.pdf

"Shecurity," Women in the Cybersecurity workforce: With women making up just 24 percent https://www.isc2.org/Research/Workforce-Study of the information security workforce, it is an imperative to focus on attracting and promoting women specifically from other fields. From a healthcare perspective, specific investment in nursing professionals should be considered (82% of RNs are women).[1] In information technology, some benefit can be gained by encouraging data analytics experts into cybersecurity roles (53% of statisticians are women).[2]

1. https://www.dol.gov/wb/factsheets/Qf-nursing.htm

2. https://www.forbes.com/sites/metabrown/2016/04/27/women-prominent-in-data-analytics-but-not-on-conference-agendas/#36c7cce82c72).

Competitions to identify candidates: This whitepaper focuses on a premise that academic educational and training programs will not be able to identify, teach, and graduate enough numbers of cybersecurity workforce members. There are additional ways to identify talent. A promising method is through competitions or cybersecurity hands-on challenges that closely relate to the real needs of employers. A compelling example - the U.S. Cyber Challenge (USCC) - is a national program supported by the U.S. Department of Homeland Security (DHS) that develops and hosts cybersecurity camps and competitions for high school, college, and postgraduate students.

The USCC consists of two complementary initiatives: The Cyber Quests online challenge series and the week-long Cyber Camp program for aspiring cyber professionals. The Cyber Quests are a set of online challenges testing basic knowledge and aptitude in information security and cover tasks ranging from secure coding to network monitoring. Based on performance in the Cyber Quests, participants are invited

to one of USCC's Cyber Camps. The Cyber Camps are week-long workshops incorporating hands-on labs, hacking competitions, and instruction by leading university and industry professionals in topics like penetration testing, packet crafting, and TCP/IP (transmission control protocol/Internet protocol) warfare. Organizations can use this model of assessment to identify and track the performance of cybersecurity candidates that may do well in on-the-job training or paid internships. Focused investment can be made to project which candidates have the desire and aptitude to take on critical work roles.

Source : https://www.csis.org/analysis/cybersecurity-workforce-gap

---

Additional References

Cybersecurity Training & Frameworks

1. Federal Virtual Training Environment (FedVTE) provides free online cybersecurity training to U.S. government employees, Federal contractors, and veterans – https://fedvte.usalearning.gov/
2. Health Sector Coordinating Council Joint Cybersecurity Working Group publication: Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
3. Information Systems Security Organization CISSP Certification – http://issa-hr.org/cissp-autumn-2017-study-course/
4. NIST'S National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework – https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework
5. Professional certificate program for Leadership in Healthcare Privacy and Security Risk Management, The University of Texas at Austin McCombs School of Business
6. Regent University Institute for Cybersecurity – https://www.regent.edu/institute-for-cybersecurity/

Additional Resources

7. 2018 HIMSS Cybersecurity Survey
8. AHA Strategic Workforce – https://www.aha.org/advocacy/strategic-workforce
9. Cybersecurity Workforce Shortage Projected at 1.8 Million by 2022 – https://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html
10. EHNAC Cybersecurity Protection in Healthcare: How Accreditation Can Mitigate Your Risk – https://www.ehnac.org/wp-content/uploads/2016/04/EHNAC-Cybersecurity-Protection-4-22-16.pdf
11. HHS OCR Cases Currently Investigation (breaches of unsecured protected health information affecting 500 or more individuals) – https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
12. HIMSS U.S. Leadership and Workforce Survey – https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_US_LEADERSHIP_WORKFORCE_SURVEY_Final_Report.pdf
13. NICE Handbook – "Cybersecurity is Everyone's Job" - https://www.nist.gov/sites/default/files/documents/2018/10/15/cybersecurity_is_everyones_job_v1.0.pdf

14. Siouxland District Health Department Workforce Development Plan – https://www.naccho.org/uploads/downloadable-resources/Programs/Public-Health-Infrastructure/SDHDWorkforceDevelopmentPlanJune2016.pdf
15. Verizon 2017 Data Breach Investigations Report – https://enterprise.verizon.com/resources/reports/phi/
16. Verizon 2018 Data Breach Investigations Report: https://enterprise.verizon.com/resources/reports/dbir

Acknowledgments

The HSCC would like to thank the principal drafters and reviewers of this resource, including:

Workforce Development Task Group Co-Chairs

Brandyn Blunt	Clinical Engineering Systems Administrator	Trinity Health
Marian Merritt	Lead for Industry Engagement	National Initiative for Cyber Education/NIST

Workforce Development Task Group Members

Dan Bowden	Chief Information Security Officer	Sentara Healthcare
Vito Sardanopoli	CISO	Independent Consultant
Sri Bharadwaj	Information Services and CISO	UC Irvine Health
Haifa AbouSamra	Chair/ Professor of Nursing	University of South Dakota Nursing School
Leanne H. Field, Ph.D.,	Clinical Professor, College of Natural Sciences, and Director, Digital Healthcare Innovation	McCombs School of Business University of Texas at Austin

Additional Review

Chris Riedel	CEO	Connectsx

Members of the HSCC Cybersecurity Working Group Workforce Development Task Group

Susan Skochelak	Group Vice President, Medical Education	American Medical Association
Nidhi Luthra	CISO & AVP IS Security and Compliance	AMITA Health
Deidre Rodriguez	Staff VP Privacy & Compliance	Anthem, Inc.
Jeff Bontsas	VP, CISO	Ascension
Vito Sardanopoli	CISO	Independent Consultant
Anahi Santiago	CISO	Christiana Care Health System
Theresa Meadows	SVP & Chief Information Officer	Cook Children's Health Care System
Michael Pry	Director, Enterprise Risk Management	Excela Health
Laura Alfredo	SVP & General Counsel	Greater NY Hospital Association (GNYHA)
Michael Miller	IT Security Administrator	Henry County Hospital, Inc
JoAnn W. Klinedinst	Vice President, Professional Development	HIMSS
Sharon Finney	CISO	Johns Hopkins All Children's Hospital
Jason Johnson	Information Security Officer	Marin General Hospital
Marian Merritt	Lead for Industry Engagement	National Initiative for Cyber Education/NIST
Brent Edington	Director, Information Systems	Pomerene Hospital
Sean Patrick	Director, IT	Ridgecrest Regional Hospital
Sheila Whalen, DNP, RN-BC	Clinical Integration Program Manager	Rush University Medical Center
Dan Bowden	Chief Information Security Officer	Sentara Healthcare
Wayne Howell	Director, Medical Equip. Tech & Compliance	Trinity Health
Brandyn Blunt	Clinical Engineering Systems Administrator	Trinity Health
Jeffrey Tully advisor)	Anesthesiology Resident	UC Davis Medical Center (independent
Sri Bharadwaj	Information Services and CISO	UC Irvine Health
Christian Dameff advisor)	Clinical Informatics Fellow	UC San Diego Medical Center (independent
Haifa AbouSamra	Chair/ Professor of Nursing	University of South Dakota Nursing School
Leanne H. Field, Ph.D.,	Clinical Professor, College of Natural Sciences, and Director, Digital Healthcare Innovation	McCombs School of Business University of Texas at Austin
Robert Bastani	Branch Chief, Information Planning & Policy	HHS Office of Assistant Secretary for Preparedness and Response

For more information about the Healthcare and Public Health Sector Coordinating Council's Cybersecurity Working Group, please see https://HealthSectorCouncil.org or contact Executive Director Greg Garcia, at greg.garcia@HealthSectorCouncil.org

##