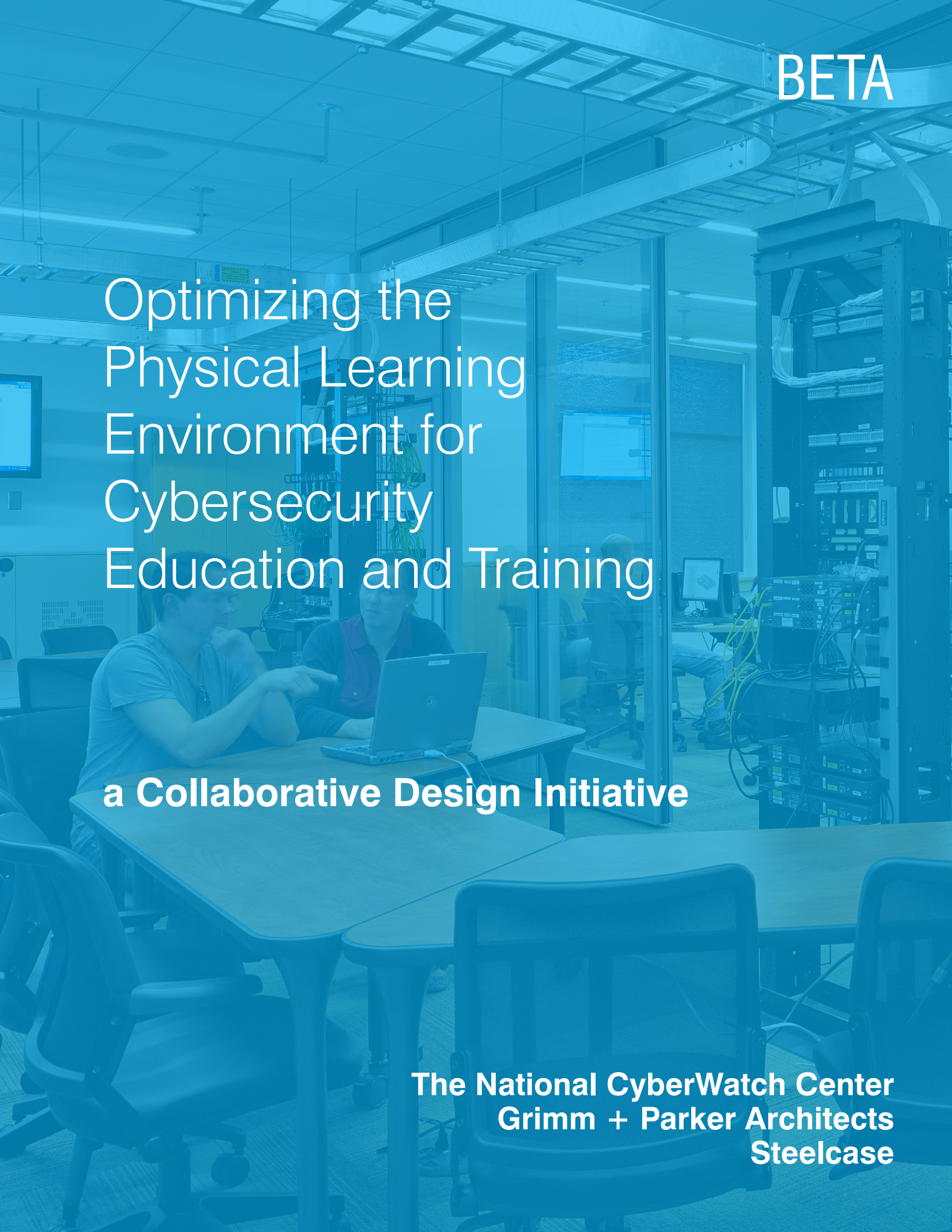


BETA

Optimizing the Physical Learning Environment for Cybersecurity Education and Training

a Collaborative Design Initiative

The National CyberWatch Center
Grimm + Parker Architects
Steelcase


G+P
GRIMM AND PARKER


national
CyberWatch
center


Steelcase
EDUCATION

contents

Executive Summary

This report is intended as a resource to the cybersecurity community offering support in the planning and design of advanced, high performing cybersecurity learning labs. The findings here are the result of a collaborative initiative undertaken by the National CyberWatch Center, Grimm + Parker Architects and Steelcase.

CyberWatch is a National Science Foundation Advanced Technological Education-funded cybersecurity consortium headquartered at Prince George's Community College, near Washington DC. CyberWatch leads collaborative efforts among schools, government and private industry to advance cybersecurity education and strengthen the national cybersecurity workforce.

Grimm + Parker Architects are experts in the design of learning environments for K-12 and Higher Education. Also located in the metro DC area, Grimm + Parker has designed hundreds of projects across the spectrum of education from kindergarten to graduate school and workforce development.

Steelcase is a global leader in the design and manufacture of furniture solutions for the workplace and education. Steelcase is recognized for its future-focused research on how learning takes place and how furnishings and planning can support effective and inspiring learning environments.

Cybersecurity is a new and burgeoning field of study and practice. Workers with cybersecurity skills are critical to protecting the digital infrastructures on which much of modern society is built. Myriad resources and programs exist addressing teaching, competencies and the workforce need. However resources to guide the planning and design of physical spaces for education and training are lacking.

Recognizing a need and using the National CyberWatch Center network, our team developed a four step process to address it. Steps one through three are complete and consist of an online survey, benchmarking interviews and site visits to gather the information that has resulted in the initial findings and recommendations published here. Step four closes a feedback cycle. We now offer this beta version of design considerations and strategies back to the community for comment.

It is our intention that this document is broadly distributed after the first feedback cycle, but that it remains a living document – adapting to a complex and ever changing cybersecurity landscape.

- Anthony Lucarelli, AIA
Grimm+Parker Architects

A fundamental, unifying finding…is that active, collaborative learning experiences that emulate real work circumstances, conducted in a dynamic physical learning environment capable of supporting team activity, are desirable if not essential to cybersecurity education.

Purpose

The purpose of this initiative is to provide a web-based resource to the cybersecurity community offering design considerations and strategies to support the planning and design for high performing, specialized, cybersecurity learning labs.

Recognizing a Need

Significant progress has been made in the pursuit of a national goal to increase the quantity and quality of the information assurance (that is, cybersecurity) workforce. A broad network of partners across the cybersecurity landscape in government, academia, and private business are consolidating policy, standards and metrics for success. Curricula, training programs, and tools and activities for teaching continue to evolve and improve, in tandem with understanding and emerging consensus around the competencies required to meet diverse workforce needs. The National Initiative for Cybersecurity Education and it's National Cybersecurity Workforce Framework* is a current case in point.

This report poses the question: For a given cybersecurity learning experience, what is the optimal physical learning environment for both space and technology? A great deal of readily available resources exist supporting workforce certifications, curriculum design, faculty development, and even strategies to develop a mature cybersecurity workforce structure in an organization – business or institution.* However, resources to guide the planning and design of the physical space for education and training are lacking.

Of course, cybersecurity workforce competences run the gamut from policy and ethics, to research incident response and forensics. Recognizing that much can be accomplished in a seminar room or simple computer lab, this initiative is focused on the most highly specialized competencies and learning experiences that may make the most demands on the learning environment – such as in virtual and simulated exercises, battle labs, research, competitions and gaming. In addition, the focus of this initiative is on the needs of higher education.

A great deal of readily available resources exist supporting workforce certifications; curriculum design; faculty development; and even strategies to develop a mature cybersecurity workforce structure in an organization, business, or institution.

However, resources to guide the planning and design of the physical space for education and training are lacking.

A Hypothesis

There is broad consensus across the educational spectrum that project based, active learning experiences are critical to powerful and lasting outcomes. Planners and designers, if not institutions and faculty, have kept pace with innovative and creative solutions integrating space, technology and furniture to support such experiences. Our hypothesis has been that the now familiar design characteristics of a “technology-rich, immersive, active learning space” may, via simple adaptation (a fundamental feature), provide an exceptional solution for a high performing cybersecurity learning lab.

Recent design exercises and observations by our team and others suggest that such adaptations may not, however, be so simple. Questions arise:

Are colleges, universities and other organizations creating new space or adapting existing space for cybersecurity? In either case, how are they doing it?

What is the extent of the need for active learning in cybersecurity – particularly given the preponderance of 100% online courses?

If active, project based learning experiences are desirable or preferred, what adaptations to the familiar, active learning labs are necessary? Are these adaptations significant enough to establish a new model?

How does the model change or adapt in response to the needs and circumstances of different providers of the learning experience – Community College and 4-Year Workforce?

A Process

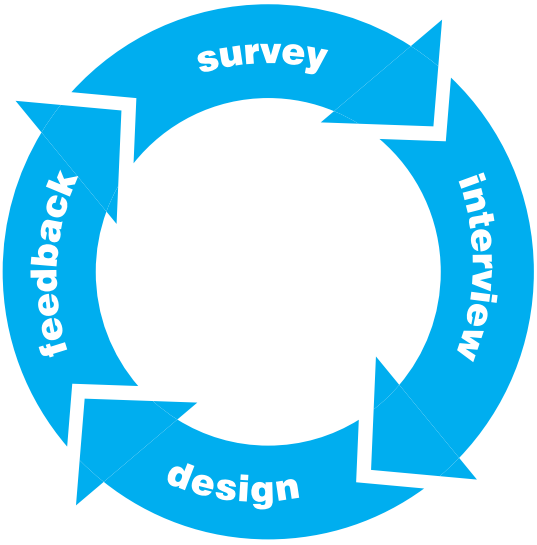
To explore answers to the questions posed above, and with the goal of producing a resource of guiding principles, design recommendations and prototypes, we established a four-step process consisting of an online survey, benchmarking interviews and site visits, design activities, and feedback.

1. The Survey: Using the National CyberWatch Center network, a survey was distributed to educators, students and professionals exploring their current circumstances and the preferred characteristics of an ideal, high-performing, advanced cybersecurity teaching lab.

2. Benchmarking Interviews and Site Visits: Using the network of colleges, institutions and businesses in the Washington, DC metro area, interviews were conducted with groups of "surrogate clients" – stakeholders who could help us interpret the survey results and envision an ideal lab that would serve their needs. In addition, existing cybersecurity learning environments were visited and studied. These interviews / visioning sessions were conducted with cybersecurity professionals and educators representing the following:

Capitol College; Northern Virginia Community College Woodbridge; The University of Maryland Baltimore County; University of Maryland University College; Northern Virginia Community College Loudoun; Anne Arundel Community College; Howard Community College; Mantech, and Cybersecurity Consulting.

3. Design Activities: Grimm + Parker Architects, in collaboration with Steelcase, produced several Cybersecurity Lab prototypes in response to the survey and interviews and created planning and design considerations, guiding principles and recommendations. These prototypes and considerations endeavor to provide the community with a vision of the design possibilities for a high performing lab, and the tools to enable them to edit, adapt and customize a vision for their unique needs.



4. Feedback: We have codified the initial results of this Cybersecurity Learning Environments Initiative and we consider this document a beta version of those results. Our next step is to solicit feedback from those involved in the initial benchmarking as well as from additional select stakeholders, consisting again of cybersecurity professionals, educators and students. This feedback will be solicited via a follow-up online survey, as well as by in-person presentation, review and comment.

findings

Survey Results

“Physical Learning Environments for Cybersecurity Education and Training”

Survey Distribution
Feb 24, 2014
Through National Cyberwatch Center network and direct email

Results Collected
Feb 24 – Apr 28, 2014
via SurveyMonkey

Demographics

120 Total Respondents

- 52% Students (2+4-year colleges)
- 31% Instructors (2+4-year colleges)
- 7% Cybersecurity Professionals

74%
from Mid-Atlantic region of US

2/3
of respondents are male, consistent through all response groups

♂
male

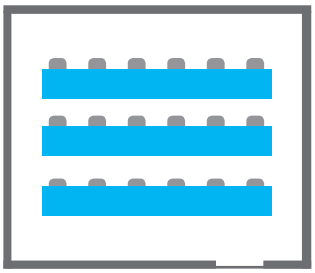
87%
of student respondents have been involved in cybersecurity less than 1 year

less than 1 year

58%
of instructors have been involved in cybersecurity more than 7 years

more than 7 years

Existing Cybersecurity Space Characteristics



A standard computer lab layout

750sf

Average area of lab space

73%

utilize a standard computer lab layout

52%

have a capacity of 20-29 students

What's working?

- ☐ IT/Technology
- ☐ Security

What's NOT working?

- ☐ Flexibility
- ☐ Furniture
- ☐ Aesthetics/Beauty

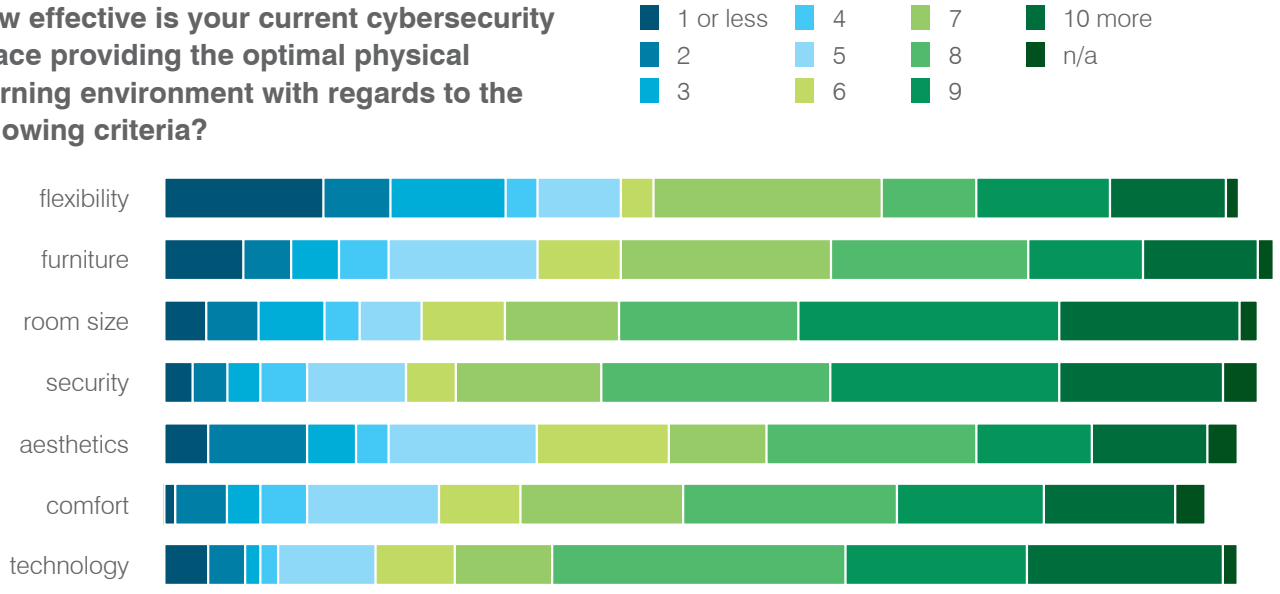
Positive Comments

IT equipment, computers and software

Negative Comments

Size, configuration and comfort

How effective is your current cybersecurity space providing the optimal physical learning environment with regards to the following criteria?



Summary

Spaces that have been retrofitted to serve cybersecurity have had most resources dedicated to IT and security updates (understandably); these criteria have resulted in highest levels of satisfaction. In most cases, using a fixed computer table layout has limited the opportunities for flexibility, collaboration and group work.

"Hard to navigate between rows to help students"

"Difficult to use BYODs in conjunction with installed PCs"

"Many grants allow equipment but not furniture and walls"

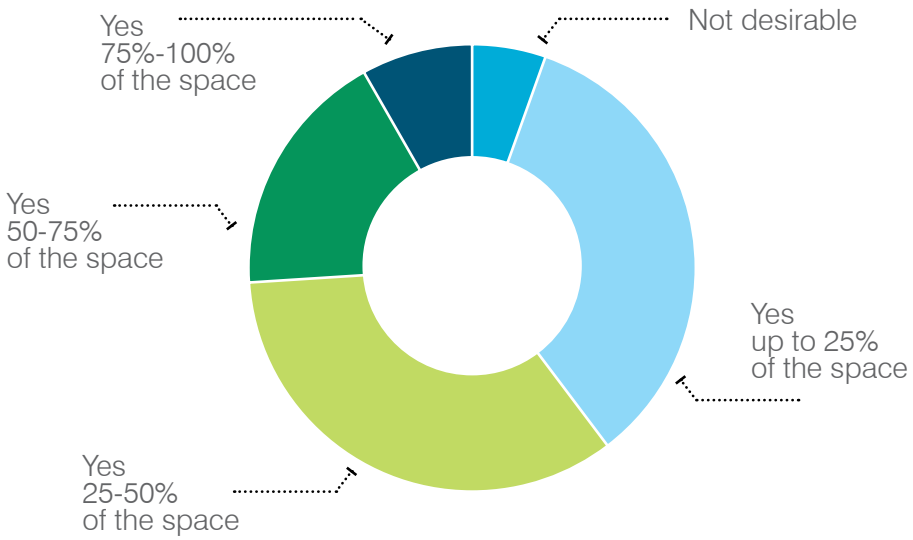
"Don't have the lab resources (techs) to maintain complex configurations"

"I would love to have a collaborative lab"

Survey Results

Future Cybersecurity Space Characteristics

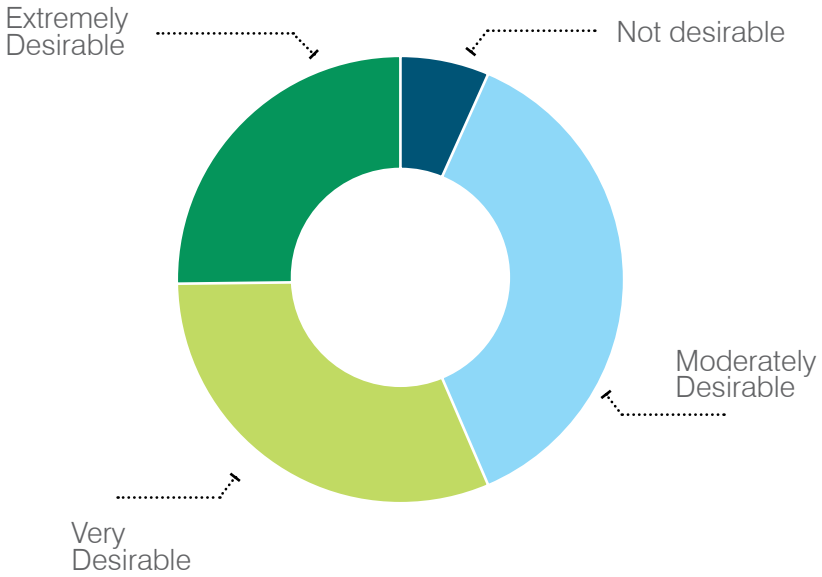
In considering an ideal cybersecurity learning environment, would it be desirable to dedicate a portion of the space or the entire space to a collaborative/project-based group environment?



95%

of respondents said it would be desirable to dedicate a portion of the space or the entire space to a collaborative/project-based group environment

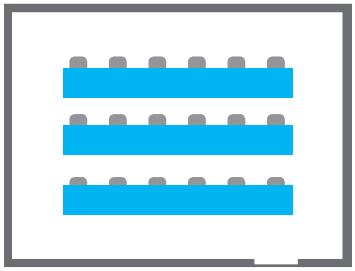
In considering an ideal cybersecurity learning environment, would it be desirable to have flexible space with furniture and equipment that could be reconfigured to provide multiple educational experiences?

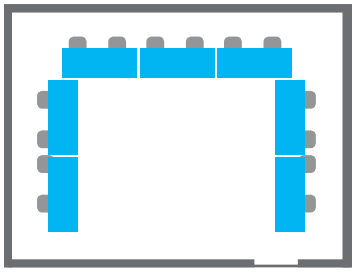


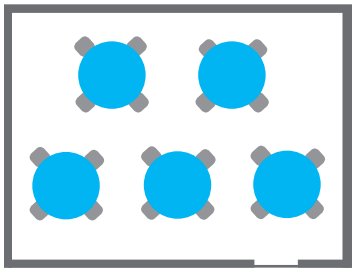
94%

of respondents said it would be desirable to have flexible space with furniture and equipment that could be reconfigured to provide multiple educational experiences

Favored Room Arrangements







Ideal student capacity

15-25
students

Ideal group size

4-6
students

Most relevant and sought-after competencies in the future

- ☐ Cyber Operations
- ☐ Digital Forensics

Most essential technology

- ☐ Hardwired & wireless networks and connectivity
- ☐ Audio/Video capture and broadcast

Appropriate Level of Physical Security

- ☐ no SCIF requirements
- ☐ Secure Working Area (SWA)

Most essential display technology

Summary

70%
of respondents said it would be essential to have a lounge space.

several
of respondents said they needed direct access to toilet rooms for 24/7 labs

76%
of respondents said it would be desirable to have interior windows to visually connect the space to the building's circulation/ public spaces and/ or showcase the programs being taught

82%
of respondents said it would be desirable to have exterior windows for views to the outdoors and/ or providing natural daylight

93%
of respondents noted the importance of the aesthetic quality and beauty of the space in providing a space that is both an effective and desirable destination for students and teachers.

"An aesthetically pleasing environment can help promote the program and will benefit the existing students"

"Open spaces…are important to showcase work being done"

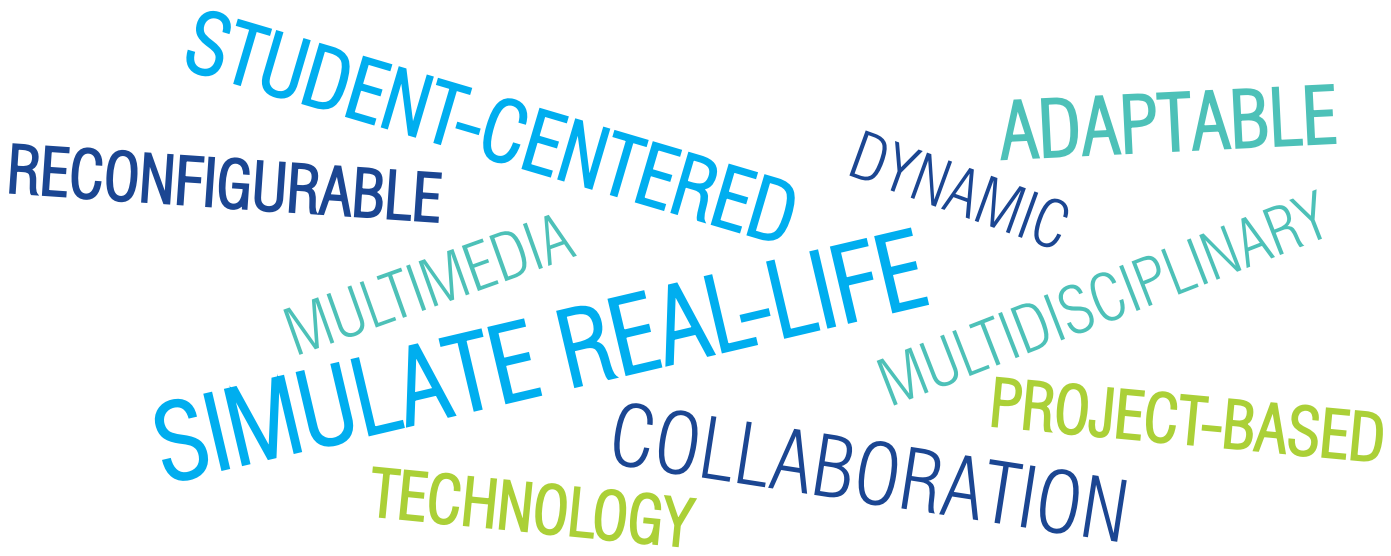
"There should be more hands on activities for individuals who learn better by doing rather than just studying."

Interviews and Site Visits

Benchmarking Existing Programs and Spaces
Interviews with cybersecurity educators and cybersecurity professionals were conducted to provide insight into the survey results, and to derive consensus around a set of fundamental recommendations for the planning and design of high performing labs. Community colleges and four year institutions with mature programs were represented, as were several private sector cybersecurity consultant firms. Like the survey, however, the majority of the participants represented community colleges, which are on the frontline of training both the emerging and the incumbent workforce. Multiple facilities were visited and studied as most college programs have, over the past 5 years, developed new or renovated cybersecurity labs.

Participants Readily Envision an Active Learning Model
Focused on Experiences + Technology

A fundamental, unifying finding from the benchmarking exercises is that active, collaborative learning experiences that emulate real work circumstances, conducted in a dynamic physical learning environment capable of supporting team activity, are desirable if not essential. Indeed, the common benefits attributed to such experiences and the spaces that best support them strongly apply to cybersecurity education and training. These attributes are desired among administrators and educators and increasingly expected by students:



Why do these attributes apply to cybersecurity, a discipline that is commonly portrayed as cellular work by individuals at a computer?

The Science of Learning:

Even though many critical cybersecurity competencies may ultimately be applied in the workforce by individuals working alone with computers, the most powerful and lasting way to learn those competencies is via active learning experiences in a collaborative group setting.

Place vs Cyberspace:

Most cybersecurity professionals work in cyberspace, but cyberspace permeates every square foot of the modern work "place." There is a need, often a critical one, for advanced cybersecurity competencies every place there is a computer and in all aspects of organizational structure and operations – from basic strategy and policy, to the physical network, to the behavior of individuals and teams.

Active Learning Experiences Best Emulate Real-work Circumstances:

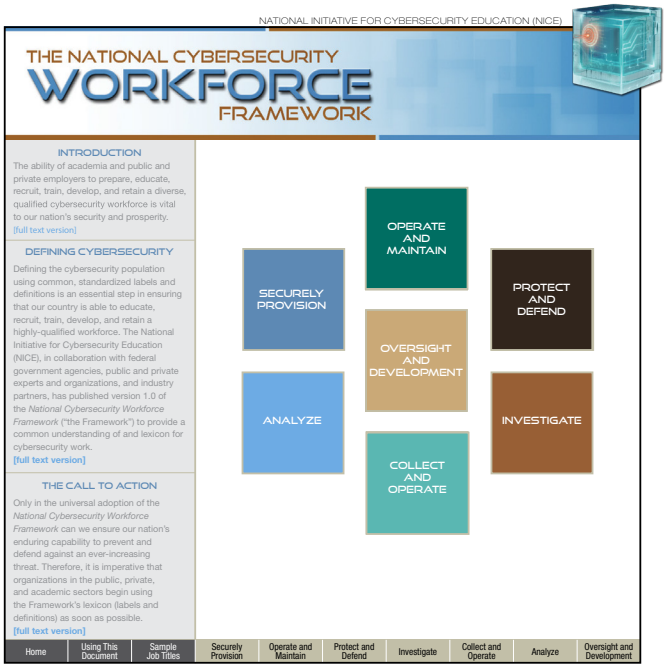
Workers with cybersecurity skills are critical to protecting the digital infrastructures on which much of modern society is built. Industries as diverse as retail, healthcare, manufacturing, and energy all depend on the security and reliability of cyberspace. With the nation facing new and dynamic risks, threats, and vulnerabilities, a highly skilled cybersecurity workforce capable of responding to these challenges is needed now more than ever.

There is a need, often a critical one, for advanced cybersecurity competencies every place there is a computer and in all aspects of organizational structure and operations.

A New, Evolving Discipline

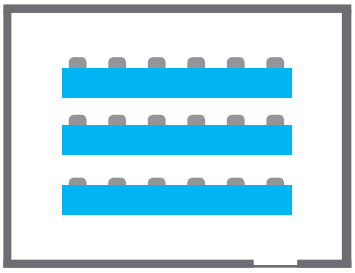
Cybersecurity is in its infancy.
There is no longstanding and uniformly understood body of knowledge to be learned or taught. There is no analogy in cybersecurity education to a cadaver in medical school, where, in the context of a lab, an entire organism may be at least fundamentally understood as a whole. Cybersecurity professionals work with corporate, institutional and government networks which are highly complex and include software, multiple hardware components, and imperfect users. Advanced cybersecurity labs need to support a range of activities from hardware repair and forensics, to exercises which test the operational readiness of a team to recognize threats and protect systems against attack while managing the complex and inconsistent use of those systems.

The Cybersecurity Workforce Framework has become the “bible” for many education and training programs. The breadth and depth of the Framework parallels the breadth and depth of the need. The Workforce Framework is a resource that categorizes, organizes, and describes cybersecurity work. The National Initiative for Cybersecurity Education (NICE) developed the Workforce Framework to provide educators, students, employers, employees, training providers and policy makers with a systematic way to organize the way we think and talk about cybersecurity work, and what is required of the cybersecurity workforce. It lists and defines 32 specialty areas of cybersecurity work and provides a description of each. Each of the types of work is placed into one of seven overall categories. The Workforce Framework also identifies common tasks and knowledge, skills, and abilities associated with each specialty area.



How are colleges responding?
Despite NICE and its Framework, cybersecurity education and training is a new, dynamic and highly valued enterprise – as such, standards are evolving and there is not yet a high degree of consistency across the industry. Colleges and universities are responding to the need in proportional ways. In general, two-year colleges are attending to technical skill development while four-year institutions are able to address business processes, research, team-building and leadership. However, ideal cybersecurity labs may not differ considerably across the spectrum of users because of similar pedagogies, the need for the labs to serve multiple disciplines, and because many community colleges are serving local business and the incumbent workforce which may make more complex demands on the labs. Blended learning models are increasingly at play given the cost of space and the amount of space required per student in high-functioning active learning environments, which can serve as hands-on supplements to online programs.

Our interviews and site visits corroborated the survey results, demonstrating that most spaces devoted to cybersecurity education and training in colleges and universities are renovations or retrofits of existing space. These labs, as well as the new, custom-built cybersecurity labs that were studied for this initiative are for the most part indistinguishable in appearance from standard and familiar college computer labs – rows of desks with one computer and sometimes two monitors at each station.



There is no longstanding and uniformly understood body of knowledge to be learned or taught.

Summary | Enhancing the Response

Features of Interest in an Improved Advanced Cyber Security Lab

Many of the programs studied have a need for what one college named a "super lab" – a lab that can accommodate a variety of learning experiences addressing a wide range of competencies from basic technical skills to forensics and research. A flexible, high performing multi-functional lab is preferred to a "specialized" or limited lab because it is easier to scale down than to scale up. This inquiry addresses such a lab.

Unifying Themes

- Design to create robust technology infrastructure – capable of supporting frequent, rapid reconfiguration of wired networks which are closed with complete integrity internal to the lab; and with the capacity for supporting extensive virtual networks. These virtual networks are the media for skill development, research and testing, and they make possible the emulation of authentic work scenarios.
- Design to support scalability of networks – with quick and easy access to servers and cabling infrastructure having considerable capacity and room for growth.
- Design to support both individual and group work as well as lecture – "all eyes on the teacher."
- Design to support work not only in cyberspace created on the virtual networks, but on the hardware itself – bench space with storage.
- Design to support reconfigurable furniture arrangements – accommodating varieties of activities and exercises, including competitions and games which may require observation and control from outside the lab by lab managers / faculty.
- Design to support adaptability in response to changing technology, changing workforce, and changing market demands.
- Design to support student expectations – dynamic, real-world and giving pride of ownership in a space that is inspiring and aesthetically appealing.

Differentiating Themes

- Lab size: Varies based on the need and the nature of the education and training programs. Large group instruction space may be justified by workforce development programs or demand on campus.
- Hardware vs. Software: The nature of the competencies being learned may demand more or less bench space in addition to computing space. Forensics programs, for example, may demand significant bench space, storage and specialized equipment.
- Underfloor vs. Overhead Cable Infrastructure: The extent and frequency of network construction and reconfiguration as well as the frequency of furniture reconfiguration within the lab may influence the choice.
- Laptop, CPU or All-in-one: The choice of computing devices influences furniture and flexibility in the lab.
- Reconfiguration: The frequency and the extent to which space can be reconfigured varies based on the institutional culture and programs.
- Ownership: Cybersecurity programs must be thriving to justify exclusive ownership by a department – particularly in community colleges. Cybersecurity labs may also need to function as advanced learning labs for any discipline.
- SCIF - "Secure Compartmentalized Information Facility": Most facilities for higher education can manage without a SCIF. Workforce development programs and facilities meant to serve the intelligence and DoD community may, however, benefit from having a SCIF.
- Server Rooms: Depending on programs and learning activities, access to servers varies from locked-away, to behind glass and accessible, to mobile racks within the lab.

Aesthetic Quality of the Inventory

Like many working emerging programs that are in high demand, faculty and students of cybersecurity tend to "make do" with adaptations and sometimes extensive renovations of existing space. Such is the case with many of the entities involved in this initiative thus far. Custom designed cybersecurity labs tend to be most common in private business and government / DoD agencies. Few colleges have custom facilities, but several have new labs in the pipeline.

What does the community want in the look and feel of the lab experience?

Natural light
Human comfort
Welcoming spaces
Inspiring innovation and exploration
Attractive to prospective students and faculty

The "image and character" that can be associated with the new college labs studied here can be described as simple, clean and "high tech." Many of the renovated labs have an "ad hoc" or makeshift appearance which in some cases may seem consistent with the notion of a "hacker culture." These conditions are understandable given the priority on technology in a cybersecurity lab.

However, recent research on learning and student expectations clearly demonstrates that the physical, aesthetic qualities of a learning environment have a role to play in student success.

Can more attention to aesthetics improve the effectiveness of the lab?

Would a different aesthetic shift a program's demography - attracting more women, for example?

Can a different approach broaden the appeal of the lab without sacrificing performance?

Many of the renovated labs have an "ad hoc" or makeshift appearance which in some cases may seem consistent with the notion of a "hacker culture"

design recommendations and considerations

Design Considerations and Recommendations

The design recommendations outlined here have been developed as a reaction to the survey and interview benchmarking findings, and are provided as a beta version – for review and comment by members of the cybersecurity community at this pre-final step in the process of publishing a web based tool that will be broadly available. These recommendations are not intended as detailed design guidelines, but rather are principles and considerations that require a design response with refinement for a given circumstance. The specific types of learning activities likely to take place in the lab may best recommend the design strategy. It is clear that as a relatively new discipline, cybersecurity is a dynamic and fluid enterprise. Therefore, this tool will be a living document, intended for adaptation and improvement as the discipline changes and matures.

The following general principles have overlapping and synergistic characteristics and considerations. Specific responses to a given principle will likely apply to others.

Flexibility, and Then Some

Flexibility and adaptability are given features in a progressive, technology-rich active learning environment. In cybersecurity education, learning space which adapts to new technology and evolving expectations in the workforce is not just an aspiration, it is a necessity.

- Significant change of room configuration, including computer stations, should be accomplished within a few hours – accommodating multiple scenarios and multiple modes of learning, per course, program or event.

- Provide large displays (fixed or mobile) and or projection to support shared viewing in any furniture configuration.

- Design to accommodate both individual, private work and group work, sometimes simultaneously.

- Plan for sizable work surfaces for a variety of student materials, tools and personal items.

- Individual computer stations are likely to require dual monitors and articulating monitor arms offering the flexibility to move the display and free-up workspace.

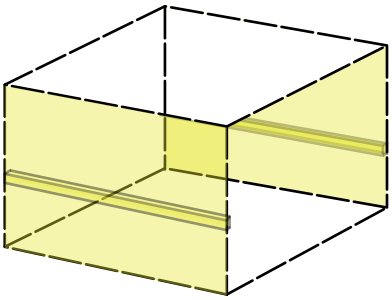
- Plan for furnishings and equipment that reliably and easily function as “plug and play” with integral wire and power management components.

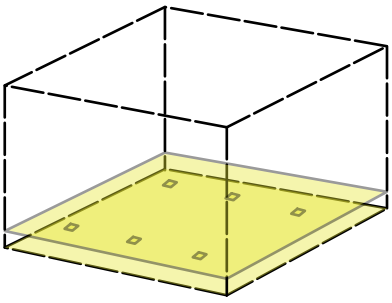
- Plan for maximum flexibility that supports “change of ownership” when circumstances warrant.

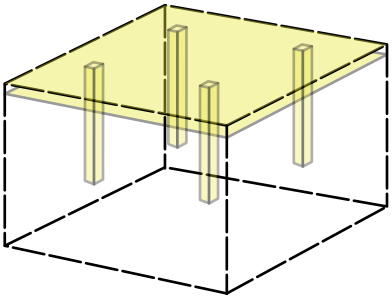
Infrastructure – Accessibility with Capacity

Infrastructure for a high performing cybersecurity lab refers to power and data – and the pathways for same. Ideally the entire perimeter of the room including floors and ceilings are designed as open chases and plenums, and server space is ample and accessible, supporting the maintenance of multiple wired (live) networks within the lab.

- Configuration of virtual networks – live computer networks replicating real network scenarios will likely become more prevalent and extensive as cybersecurity learning tools evolve.
- Re-configurability of the wired networks is as critical as the reconfiguration of space.
- Consider raised floor systems. Open raceways (cable trays for example) overhead may be desirable in research environments.
- Extensive virtual networks require significant support with servers and storage area networks (SAN). Plan adequately for space, power, storage and cooling.
- Plan for ease of access and even visibility of server racks from within the lab.
- Anticipate expansion of the networks and the elements, spaces and systems that support them.
- Plan for a control center – within or outside the lab with the connectivity to control activity on the virtual networks.
- Plan for UPS power back-up as a minimum measure.







A Physical and Social Enterprise

Cybersecurity problems are as much physical and social in nature as they are logical. Cybersecurity professionals will interact with the world of real machines and the people who use them as much as with the virtual world.

- Plan for bench space and for sometimes intensive and invasive manipulation of hardware – CPU's, handheld devices, routers, switches, hard drives etc. The flexible, multi-function lab will accommodate a measure of "shop-like" activities depending on the program.

- Specialized Equipment: if forensics focused on "extracting data" is a significant part of the anticipated learning activities, then equipment requiring special design considerations may be in play.

- Bench storage for small tools and accessories immediately accessible from the bench space is necessary to support bench activities.

- Plan for ample general storage immediately accessible from the lab for equipment, supplies, cabling and other common physical components needed for the quick and easy manipulation of the network infrastructure.

- Provide small group lounge space in or adjacent to the lab to support informal gatherings of small groups and to facilitate collaboration and communication. Include soft seating, sofas, and occasional tables.

- Provide areas and furnishings within the lab that can be manipulated to accommodate individual focused work and reflection – an opportunity for a measure of semi-privacy, as well as for team work.

- Thriving cybersecurity labs are sometimes 24/7 environments, available for student project work as needed. Consider providing supporting amenities in the lab such as a kitchenette with refrigeration.

Diverse, Multifaceted Learning Experiences

Emulating a real-world work environment or scenario in cybersecurity has expansive possibilities. More so than in most disciplines, cybersecurity competencies will be deployed across the full spectrum of strategy and operations in business, government, military and intelligence communities, and public services and utilities.

- Plan for the possibility of multiple learning zones within the lab, supporting formal, informal, individual and group activity.

- Anticipate simulated learning activities on live computer networks with role-playing virtual scenarios emulating real ones such as a common corporate network. Support intensive interdisciplinary interaction, communication and collaboration.

- Anticipate competitions such as red team / blue team activities (attack and defend) and other gaming scenarios.

- Labs or spaces within them may be configured to support and encourage student research and autonomous exploration and invention.

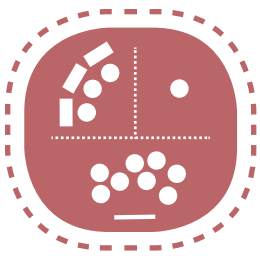
- Ancillary/Support Spaces: Consider ancillary spaces and functions outside the lab that can support variety and enrich the quality learning experiences possible within the lab. The number and size will depend on the circumstances. Note the following examples:

  Conference / Breakout: conference room for seminar, small group activity, debriefings etc. Collaboration space for small groups to remove themselves from the lab environment with direct access from the lab.

  Observation / Control: Small group space for observation (scoring) of the activities within the lab (white cell function) and to manage and control the virtual scenarios.

  Garage Band Space: A mini-lab with robust infrastructure available for students to experiment and explore network design, configuration and management - frequently a place for the intermingling of levels of expertise.

  Event Response Environment: As forensics becomes increasingly necessary in cybersecurity, some programs may benefit from a space that can be configured to replicate a “crime scene” requiring forensics investigation – a hacker’s apartment for example.



Inclusive Aspirational Vision for Design – Invite and Inspire

Learning spaces can reflect the positive and meaningful role that cybersecurity professionals will increasingly play in making secure and safe the cyberspaces that exist in every place we live, work, learn and play.

- **Aesthetics Matter:** Cybersecurity students, faculty and workers deserve comfort and beauty in the spaces where they learn. Numerous factors may be contributing to a lack of emphasis on aesthetics in the design of cybersecurity labs in higher education.

  Preponderance of renovations, retrofits and ad-hoc spaces in response to an urgent need.

  Emphasis on the cost and the "image" of technology and computing.

  Stereotypes suggesting that cybersecurity work is a reclusive, anti-social enterprise undertaken by individuals in a darkened room at a single computer.

  The cybersecurity workforce in both teaching and practice often comes out of the military service and intelligence community culture.

  The perception that all cybersecurity competencies can be learned online.

- **Comfort and Inclusion:** Spaces for cybersecurity should invite participation and stimulate curiosity among diverse users – men, women, students and professionals. Natural light, color, texture and variety are design features which are proven to help foster collaboration, innovation and exploration.

- **Image and Character:** There are abundant sources for inspiration for the look and feel of a cybersecurity lab. Interior design and material quality may be driven by the vision and mission of the college or university, the local community, and the workforce or career path being supported by the programs:

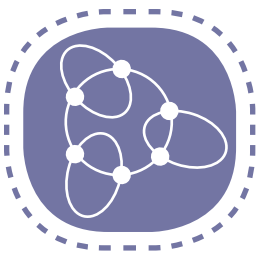
  The corporate workplace – consider the kind of work environment one might expect in a Google-like start-up versus a government contractor or consulting firm.

  The Government workplace – consider the expectations of a military facility vs. the intelligence community.

  The hacker culture – consider the possibility of reflecting the positive characteristics of the subculture referred to as "hackers" – or even "crackers." Hackers engage in activities of playful cleverness (such as in programming and other media) in a spirit of exploring the limits of what is possible and circumventing the limitations of systems. Crackers exploit weaknesses.

  Research – consider the possibilities of a research environment – specialized and precise vs. exploratory and spontaneous.

- **Celebrate and Diversify:** Ultimate success in cybersecurity – and in protecting our privacy and our critical infrastructure – lies in a diverse and highly capable workforce. Plan labs to exist in prominent locations with transparency to celebrate and display the activities and results. Design labs to inspire passion and stimulate curiosity.



Prototypes

Based on the design considerations and general principles outlined above, a team of designers from Grimm + Parker Architects and Steelcase have generated a variety of prototypical lab plans. This exercise proposes design strategies, components and features for high functioning laboratories for cybersecurity education and research. These design strategies may apply to High School, Community College, 4-year College, and Workforce education and training.

The prototypes offer a starting point for considering the functional layout with options in the configuration of furniture which is essential to the function of the labs. In addition to considering the configuration of individual labs, possible relationships among labs and supporting spaces are explored.

The goal is to provide the community a baseline scope for teaching labs of two different sizes, with optional functionality (kit of parts) adaptable to the needs of a given situation.

Flexibility

Infrastructure

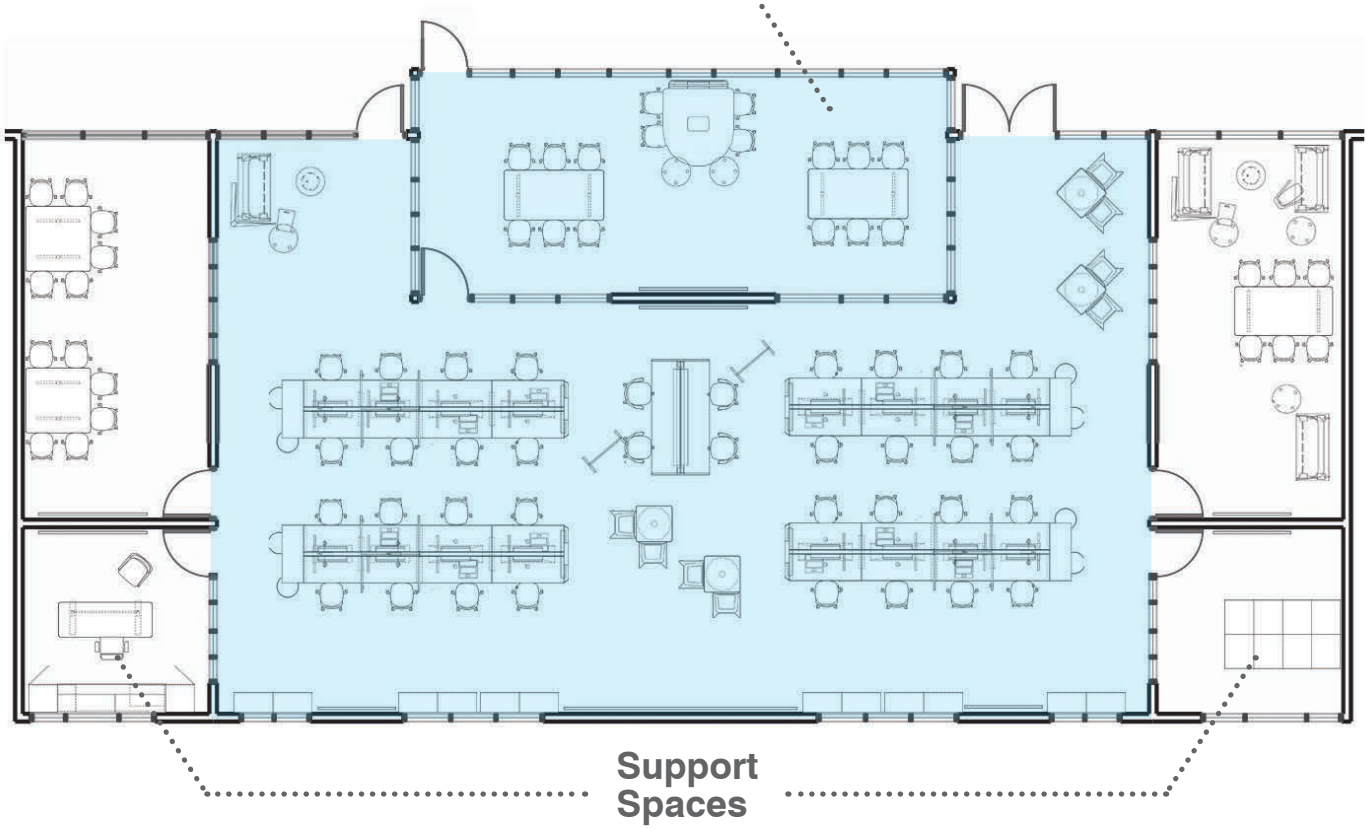
Physical+Social

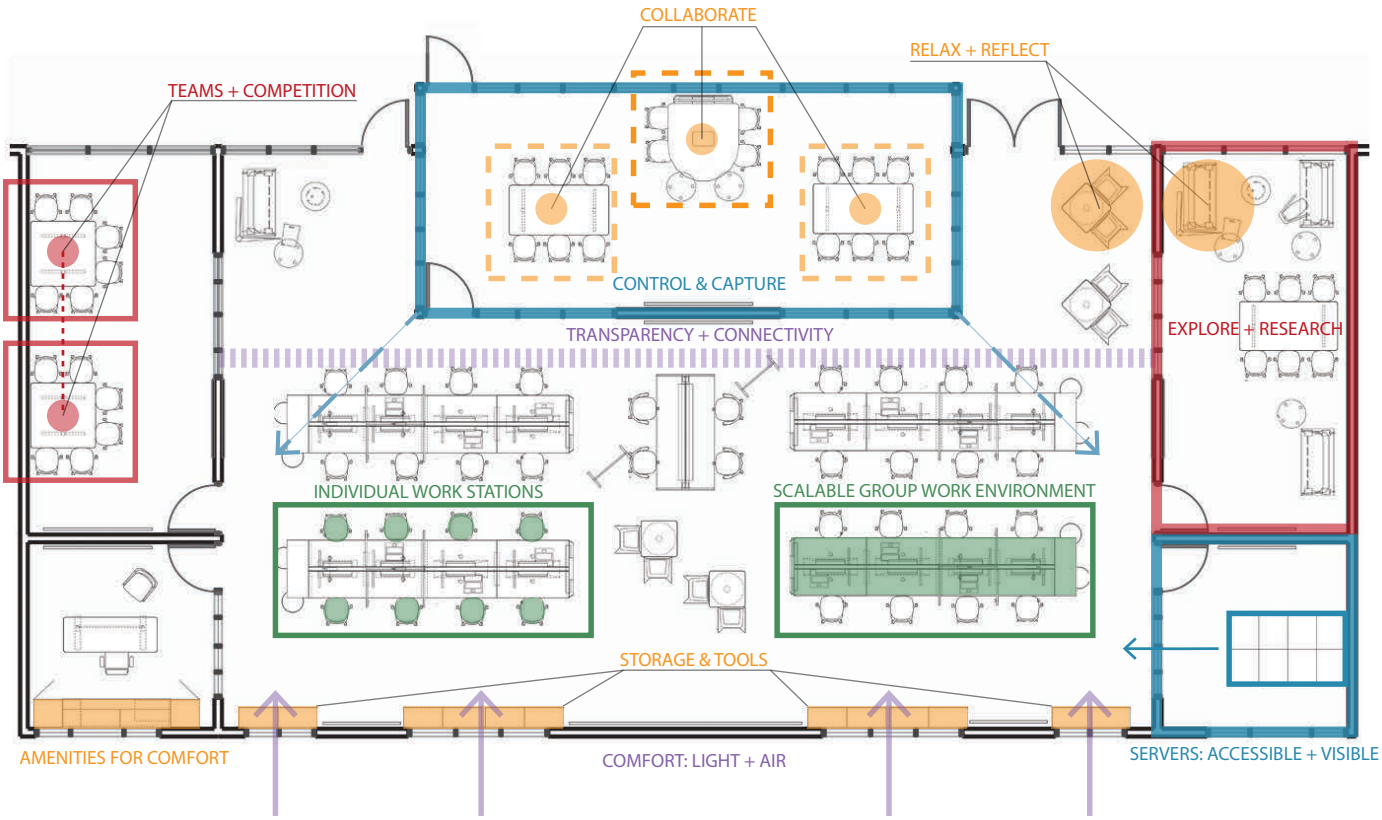
Multifaceted

Inclusive

Prototypes | Large Lab

Large Lab 2400 sf | 52 of stations

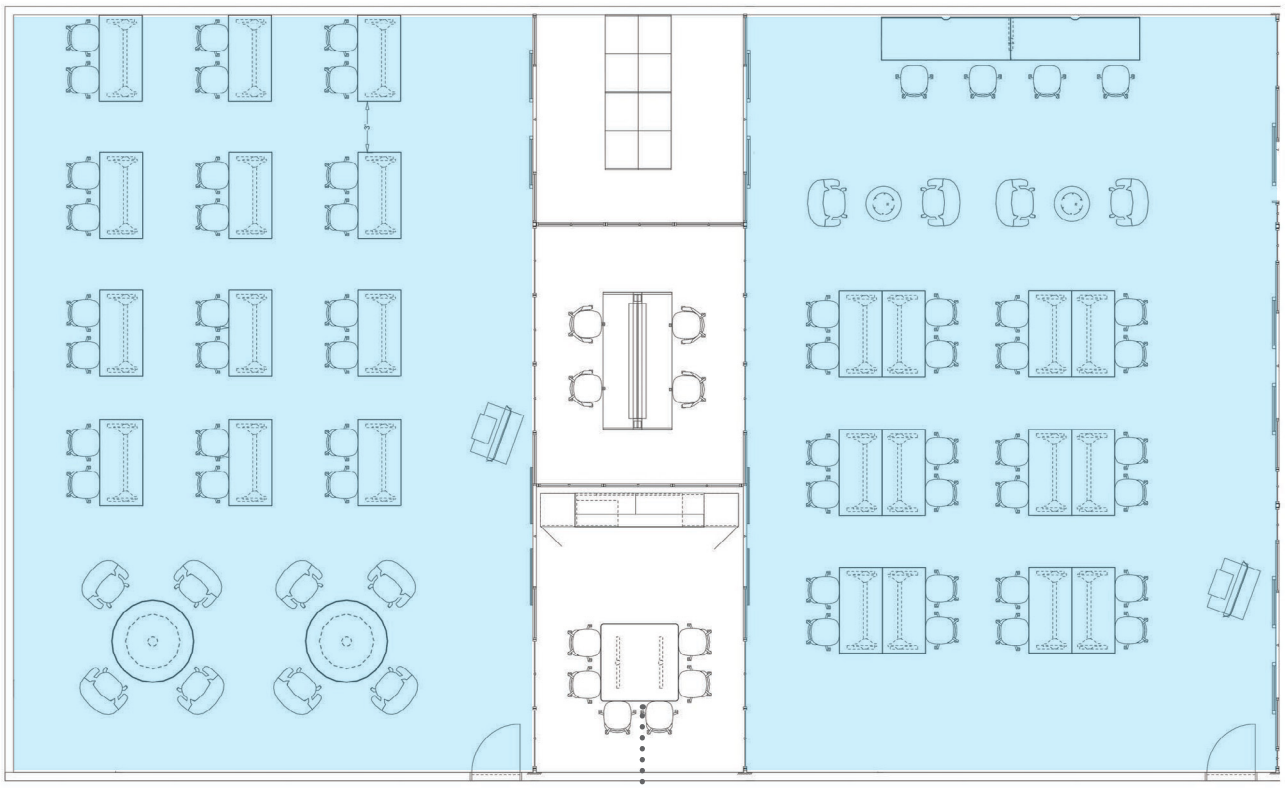




Prototypes | Small Lab

Small Lab 1 1200 sf | 24 stations

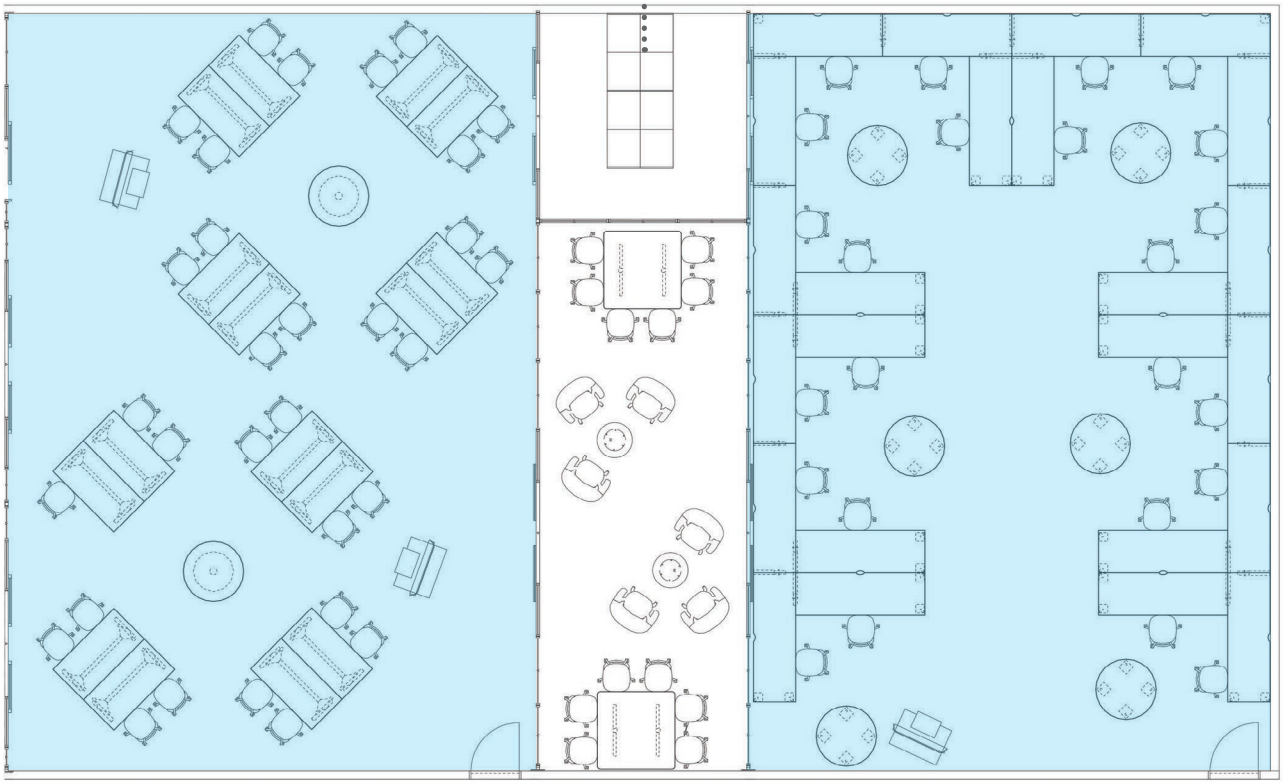
Small Lab 2 1200 sf | 28 of stations



Support Spaces

Small Lab 3 1200 sf | 32 stations

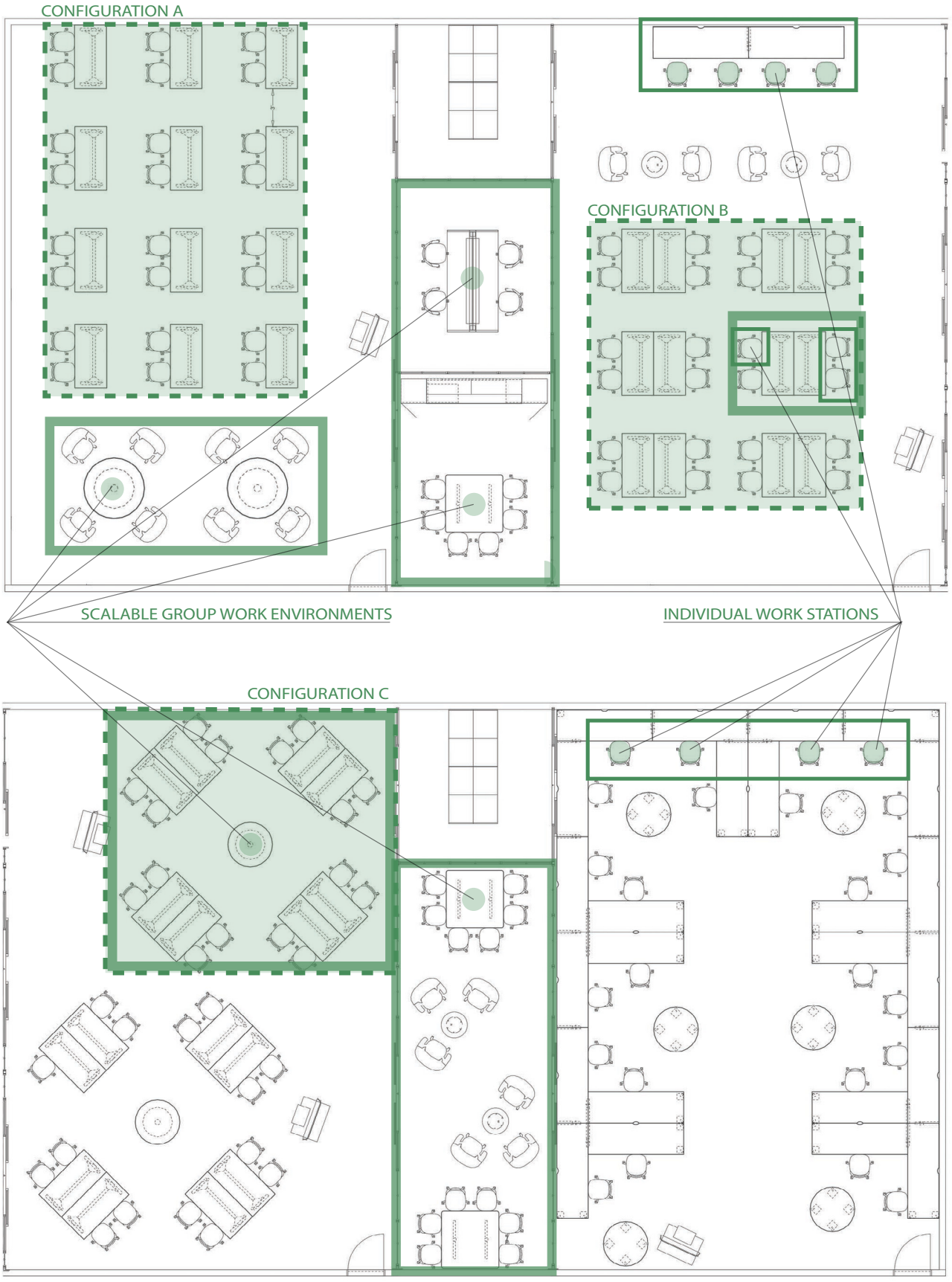
Small Lab 4 1200 sf | 24 stations



Flexibility, and Then Some

Flexibility and adaptability are given features in a progressive, technology-rich active learning environment.

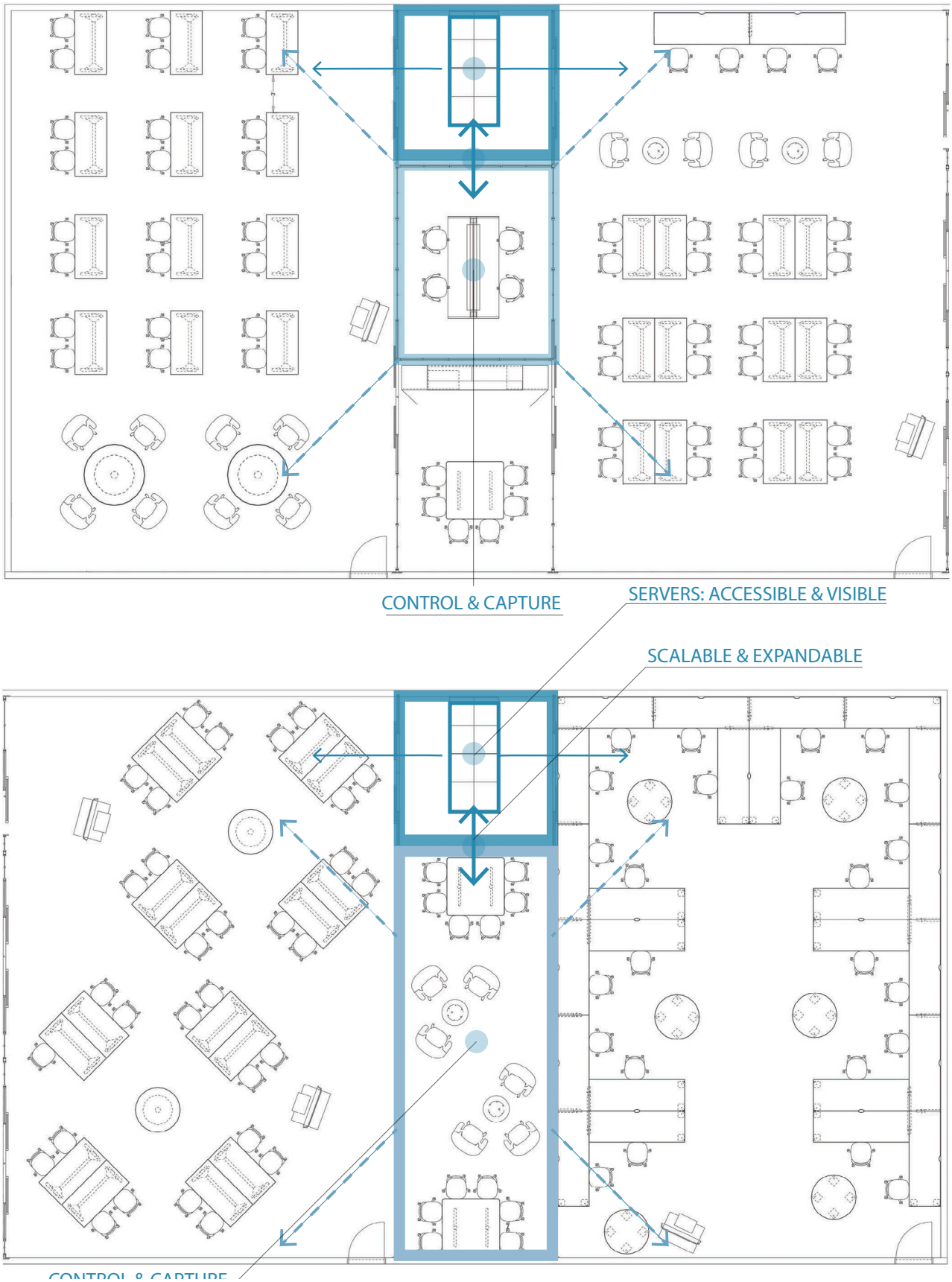
Flexibility



Infrastructure – Accessibility with Capacity

Infrastructure for a high performing cybersecurity lab refers to power and data – and the pathways for same.

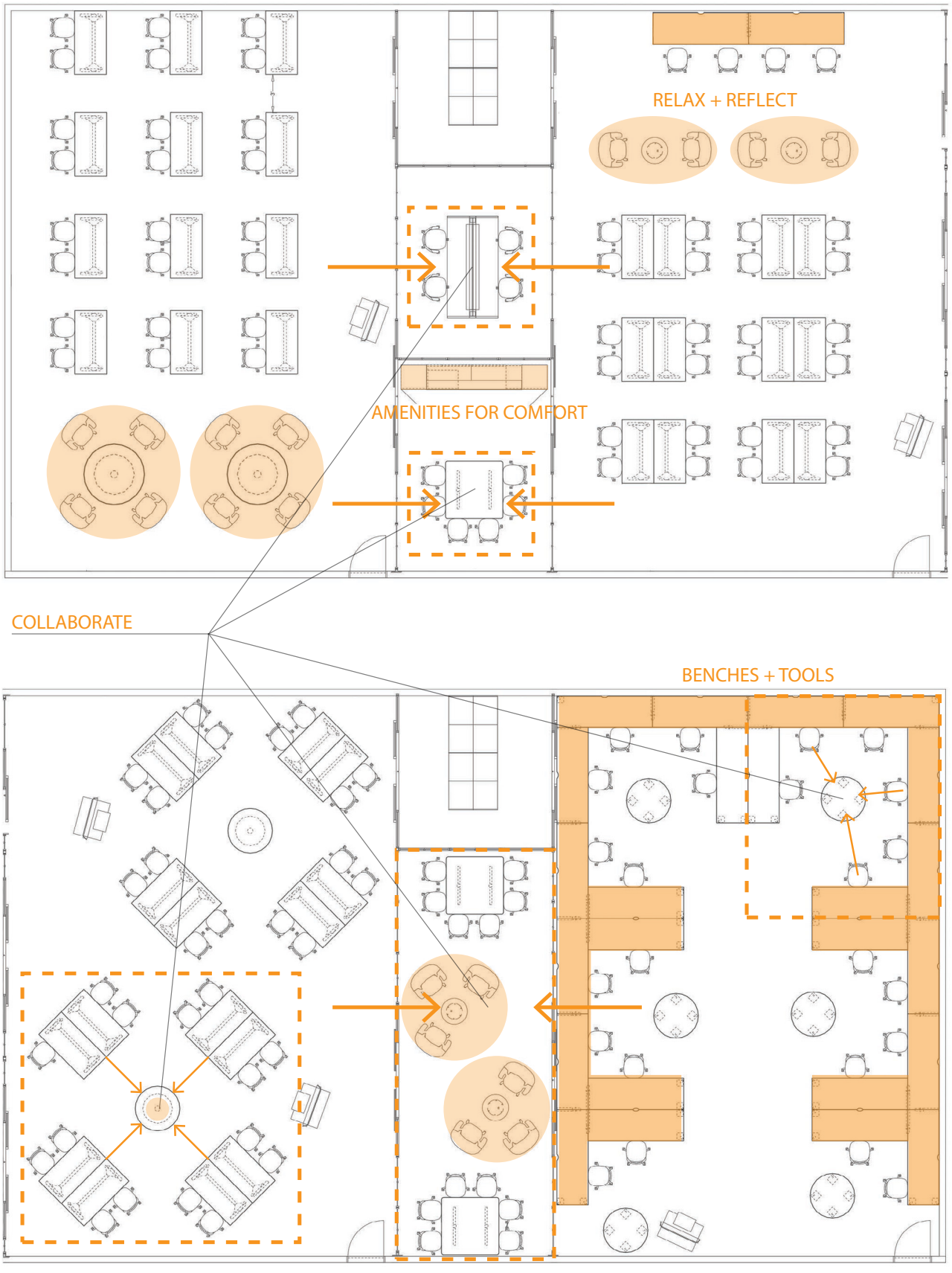
Infrastructure



A Physical and Social Enterprise

Cybersecurity professionals will interact with the world of real machines and the people who use them as much as with the virtual world.

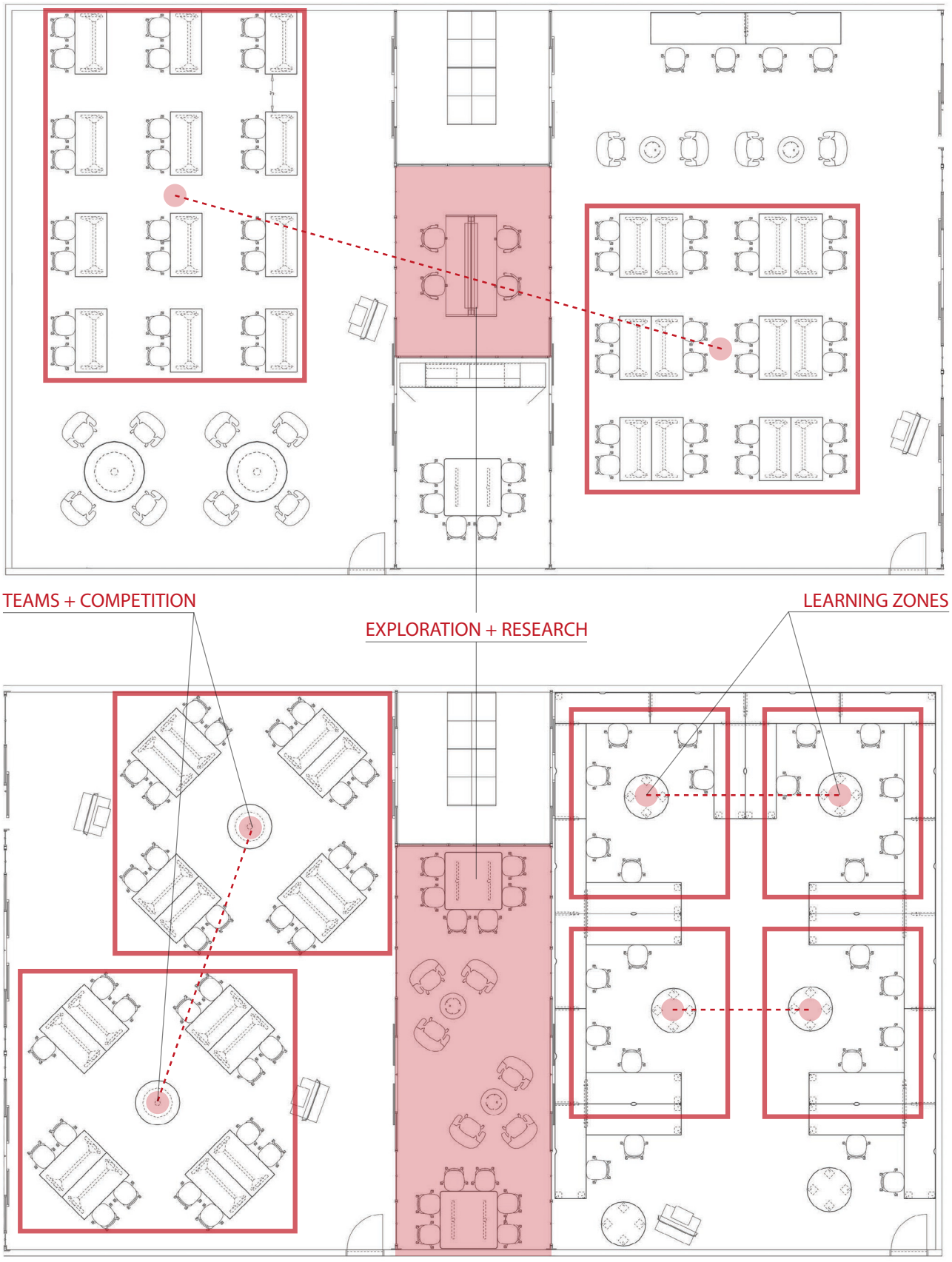
Physical + Social



Diverse, Multifaceted Learning Experiences

Emulating a real-world work environment or scenario in cybersecurity has expansive possibilities.

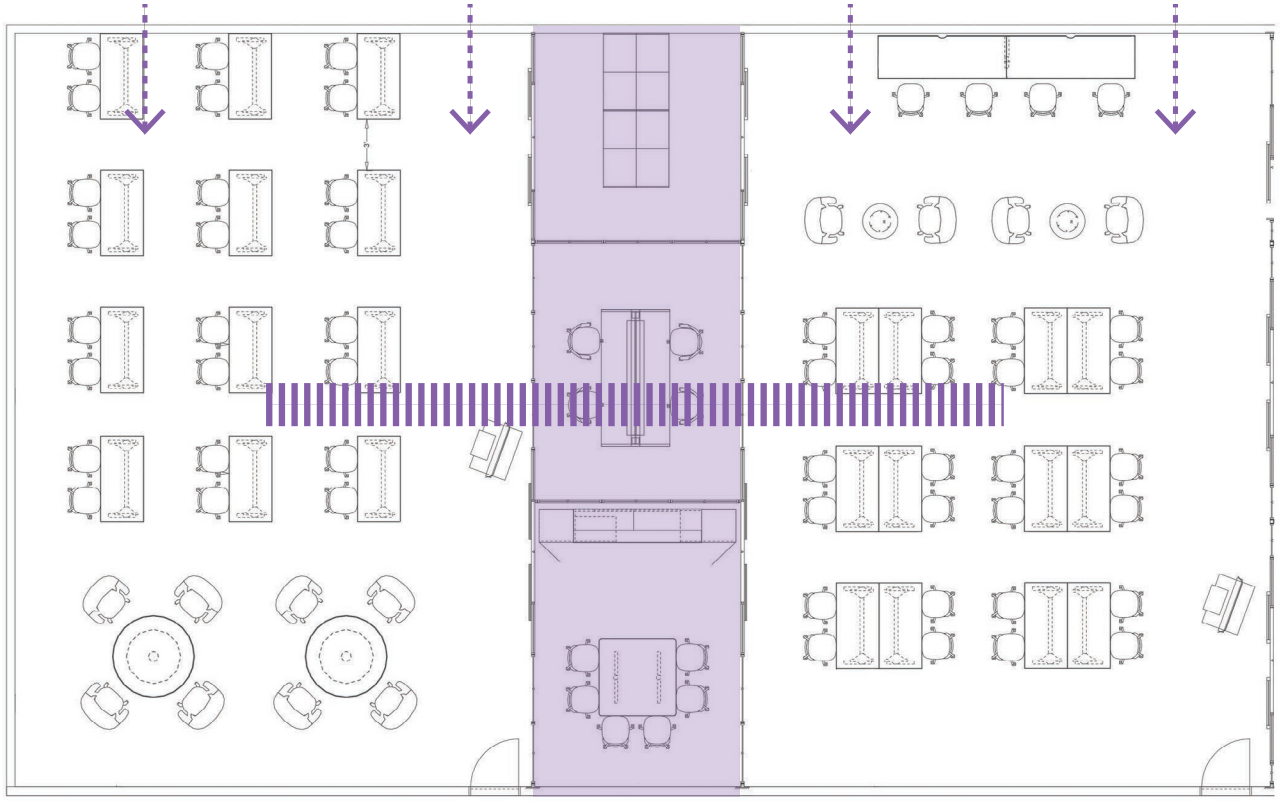
Multifaceted



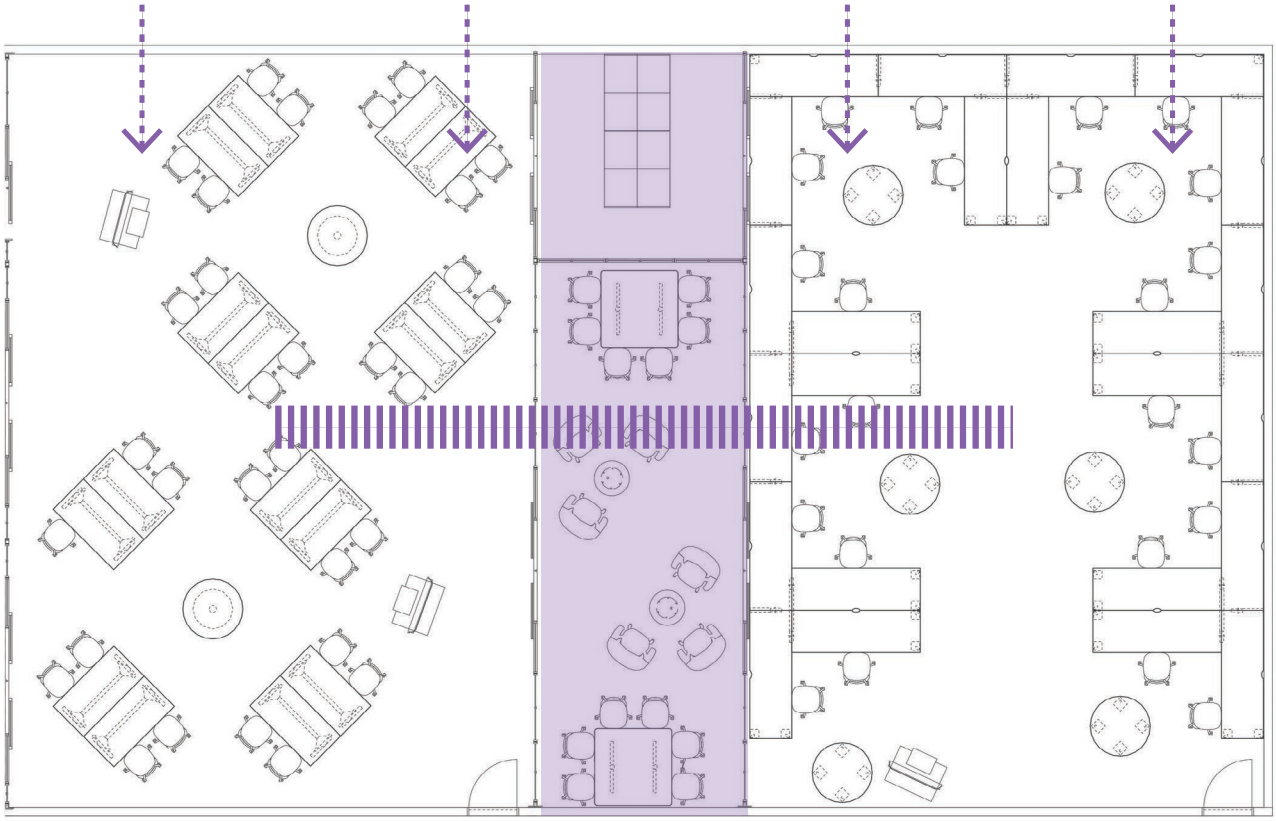
Inclusive Aspirational Vision for Design

Learning spaces can reflect the positive and meaningful role that cybersecurity professionals will increasingly play in making secure cyberspaces that exist in every place we live, work, learn and play.

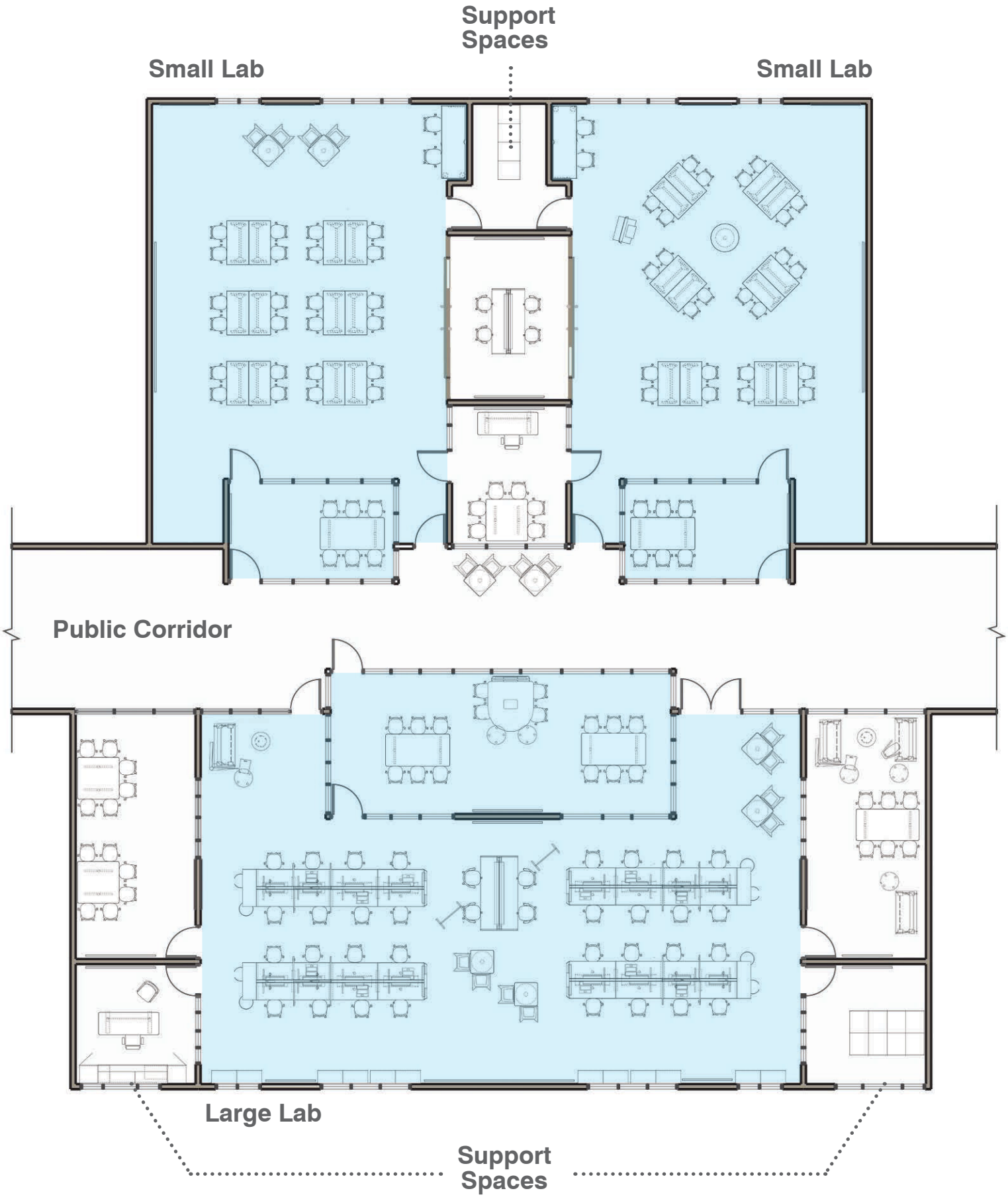
Inclusive



COMFORT: LIGHT + AIR

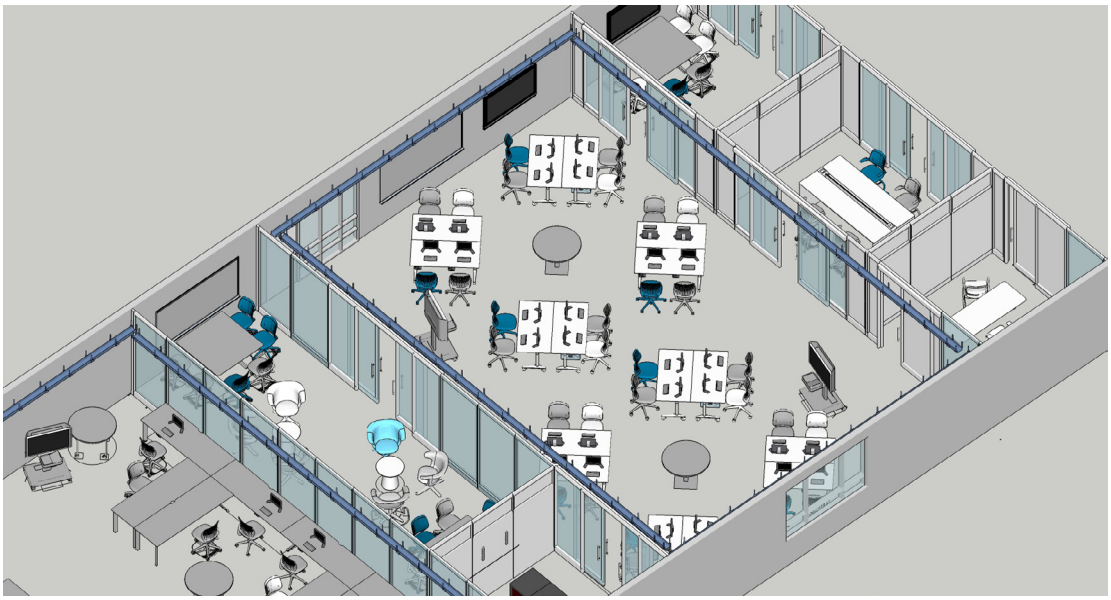


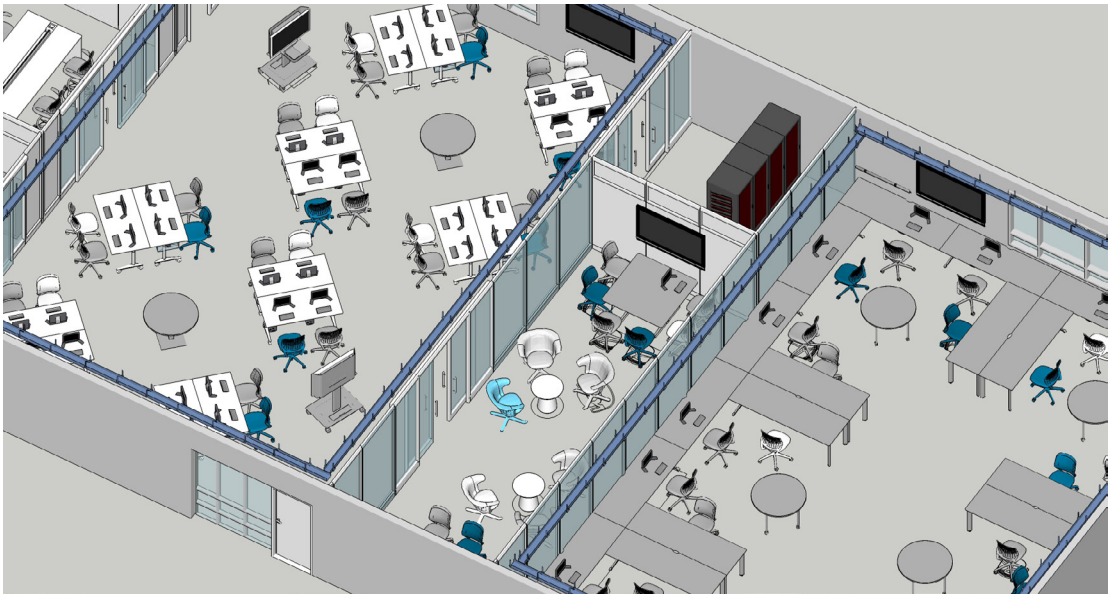
Possible Building Configuration



Next Steps

As a beta version, this document will be made available to members of the cybersecurity community in academics, government and the private sector for review and comment. In addition, the survey will be redistributed to solicit input from a broader spectrum of participants and a wider geographic reach. That survey will be expanded and refined by virtue of the findings and products of this initiative. Upon reaction to review and comment by the community, this resource will be published and made widely available via publication on the CyberWatch website.





acknowledgments

Author

Anthony Lucarelli, AIA - Grimm + Parker Architects

Contributors

Kieran Wilmes, AIA, LEED AP - Grimm + Parker Architects
Janice Szymanski, AIA - Grimm + Parker Architects
Laura Meador, Assoc. AIA - Grimm + Parker Architects
Joanna Hoffschneider - Grimm + Parker Architects
Ricardo Seijo - Grimm + Parker Architects
Ken Filler - Grimm + Parker Architects

Casey O'Brien - The National Cyberwatch Center

Cynthia Hund - Arbee Associates
Jill Houpt - Arbee Associates

Donald (Chip) McLellan - Steelecase
Chris Hanes - Steelecase

John Sener - Sener Knowledge, LLC

William Butler - Capitol College

Acknowledgments

The CyberWatch | Grimm + Parker | Steelcase team wishes to acknowledge the generous participation of the following individuals who via their expertise, passion and dedication to cybersecurity education have made this initiative meaningful:

Brian DeMuth, ManTech
George Hinckley, ABET, Inc.
William McLaughlin, Cybersecurity Consulting, NVCC Woodbridge
Joel Scharlat, IVEA Consulting
Adam Bixler, Cybersecurity Consultant
William Butler, Capitol College
Allen Exner, Capitol College
Andrew Mehri, Capitol College
Kip Kunsman, Anne Arundel Community College
Vinitha Nithianandam, Howard Community College
Jeff Tjiputra, University of Maryland University College
Robert Morris, SAIC
Chola Chhetri, NVCC Loudoun
Robert Dusek, NVCC Loudoun
Joseph Agnich, NVCC Loudoun