ADVANCED CYBER SECURITY CENTER

COLLABORATIVE DEFENSE • TRUSTED NETWORKS

2021 11TH ANNUAL ACSC MEMBER CONFERENCE

# INTEGRATED STRATEGIES FOR CYBER TALENT AND TECHNOLOGY

## BRIEFING SUMMARY: CYBER RANGES AND EXERCISES

FALL 2021

THANK YOU TO OUR RESEARCH PARTNERS:

SimSpace Randori

# I. HIGHLIGHTS

**Exercising needs to be part of every security program** – respond and recover are important parts of the NIST Cybersecurity Framework, responders need to dedicate the necessary time to practice and hone their skills – both individually and as teams.

**Tabletop exercises are becoming commonplace,** cyber ranges should follow suit.

**Few are actively using cyber ranges to assess and train their cyber teams.**

**Major U.S. banks like JP Morgan and Wells Fargo have been early adopters,** and have even brought their regulators in to observe their teams' skills.

**Military culture is built around drilling and training;** cyber ranges to assess staff and develop cyber team dynamics have become an extension of that culture.

**Collaborative range exercises are a unique ACSC program,** providing an exercise capability and a unique real-world environment to build peer networks and compare notes on standard operating procedures.

# II. WHAT'S THE ISSUE? WHY IS IT IMPORTANT?

## DEFINITION

**A cyber range is a virtual environment, a safespace/sandbox, used by staff and teams for cyber training, software development and testing.**

> **"Exercises on cyber ranges provide an opportunity to develop and assess the continuous evolution of people, process and technology."**

# III. THE CURRENT STATE OF PLAY AND CHALLENGES

## THE SECURITY CHALLENGES ARISE ACROSS PEOPLE, PROCESS AND TECHNOLOGY

### PEOPLE:

**Outside the military and major banks, few organizations have adopted effective programs to develop and assess their defender staff in realistic environments.** Sophisticated cyber ranges and exercises have been pioneered by the military and major banks in the last five years, focused primarily on training and assessing individual staff and teams. However, at most private and public sector organizations, cyber ranges and exercises are not yet a key element of their cybersecurity program.

> Few staff have the development opportunity to access this important kind of embedded, experiential training that has proven most effective in other fields.
>
> Organizations have no performance-based means of assessing their defender teams, benchmarking and developing their capacity, or in the case of outsourced security services, assessing the capacity of their managed service or security providers.

### PROCESS:

**Too few opportunities to build “collaborative defense” practice – within and across organizations and the public and private sectors – into realistic cyber incident exercises.** And while tabletop cyber incident simulations have developed internal collaborations and staff awareness over the last five years in many organizations, there are opportunities to bring non-technical staff into range exercises to expand awareness and understanding of roles during a large-scale cyber incident.

### TECHNOLOGY:

**Technology assessments are conducted separately by major customers without opportunities for peer collaboration and review, on ranges that are expensive to develop or designed by vendors to showcase their product.** Sophisticated cyber ranges used by groups of major firms as testing “sandboxes” offer an opportunity to assess new technology tools efficiently and realistically using sophisticated platforms that align to internal environments – with the advantage of sharing and comparing results.

## VAST DIFFERENCES IN CYBER RANGES

**Advanced cyber ranges are now available that are qualitatively different in their impact and capabilties.** There are vast differences in cyber ranges, from simple, static offerings to the most sophisticated, dynamic ranges that have realistic network traffic flowing through a complex IT infrastructure of a large company. Ranges can vary in size, VMs, network traffic, and the security tools. They can utilize "red teams" to attack and "blue teams" to defend in a live action event – and then come together as "purple teams" to learn full perspectives.

## BASIC "LEARNING" RANGES

**More basic "learning" ranges** can be used on a broader scale to develop low-medium level staff skills, or to train specific functions, like application developers. Smaller organizations with limited staff can start with simpler ranges to evaluate and then train on specific skills.

## CLOUD PLATFORMS

**Cloud platforms provide flexibility to quickly stand up sophisticated cyber ranges** that replicate internal environments with common devices and architecture for training staff and testing products

> "Cyber ranges can be scaled to the needs of a company, its budget and goals."

## MARKET

**The market for range-based, individual skills programs is growing.** SANS has regularly supplemented its coursework with cyber labs. Providers offer full, cloud-based course catalogues with modules targeted at specific technical skills. We also see what are called cyber gyms or cyber fitness programs tailored to 30-60 minute sessions. While some ACSC members are testing these out with voluntary offerings, our expectation is that the demand from next-generation staff for online, range-based development opportunities and the market offerings available will expand significantly in the next five years as off-site trainings lose customers in the post-COVID, remote work environment.

## DEMAND NEEDS A PUSH

**72%**

of ACSC conference session attendees reported limited or no cyber range experience or knowledge.

**44%**

of attendees said range exercises were not being used for staff and team development, and another 15% were not aware of their use.

## COLLABORATION

**Collaboration within and across organizations builds trusted relationships – and demonstrates strengths and exposes weaknesses.** Tabletop simulations and employee awareness campaigns have expanded collaboration within organizations over the last decade. Cyber range exercises can build further internal and external collaborations – especially between the government and the private sector where collaboration remains more aspiration than reality.

> **Working with outside parties shows how you are different and how you are the same; we mostly learned how we are more alike than not.”**

> **“It is critical for the military to partner with industry...cyber transcends DoD and industry; we are all in this together, the skills we need to build are the same and collaboration will help drive down costs.”**

# IV. EMERGING OPPORTUNITIES

## RANGE-BASED EXERCISES ACCELERATE INNOVATION, REDUCE COST AND IMPROVE SECURITY

| CURRENT PRACTICE | EMERGING PRACTICE |
|---|---|
| Non-technical tabletop exercises - low technical fidelity | Range-based training exercises - high technical fidelity - well-suited to emerging cloud environments |
| Single enterprise, no outside collaboration | Multiple, collaborating enterprises, including state and federal government |
| Limited range marketplace and vendor-specific platforms to assess tools | Data-driven tool aquisition, integration, assessment |
| Few opportunities to develop and assess front-line defensive teams | Significant value at all levels of the enterprise |

### DEPARTMENT OF DEFENSE

**DOD trains all their personnel regularly, so they can perform their duties no matter what, but they didn't have a training ground for their cyberwarriors.** Jeff Fisher led the effort to develop a training space. SimSpace was the main provider, developing a user-friendly range that could be adaptable and meet a wide range of exercise needs, creating a wide range of environments, from government networks to private sector critical infrastructure like power plants and water utilities. This is now the Persistent Cyber Training Environment (PCTE) and its uses include:

- Assessing individual cyberwarrior capabilities
- Training and developing cyber teams
- Expanded to developing and practicing ConOps (Concept of Operations)

## JPMORGAN CHASE & CO.

**JPMorgan Chase & Co. has invested significantly in range development for five years:**

- To engage the organization broadly and raise awareness, JPMC is shifting to smaller, more frequent exercises, instead of major, multi-day events
- Technical exercises focus on applications and operations teams vs. just infrastructure components (e.g., firewalls, directories, DNS)
- JPMC has built a library of online courses and has shared them with Historically Black Universities and Colleges to attract new talent

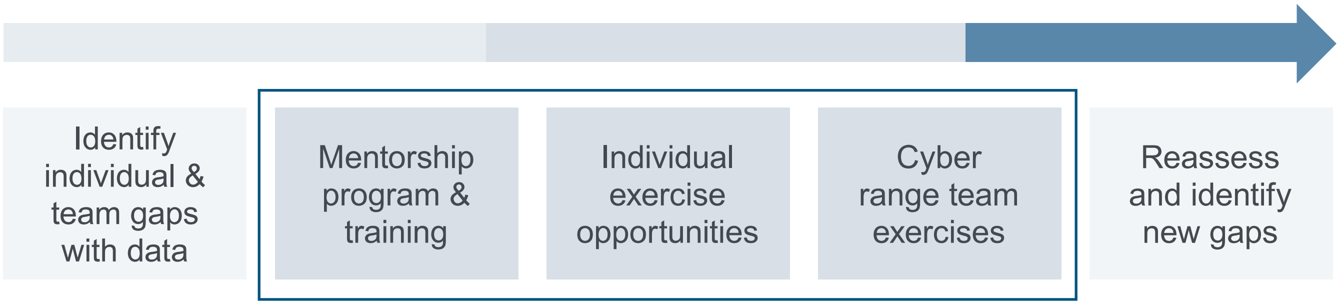
## SIMSPACE

**SimSpace case studies from military and financial clients documented:**

- Improved readiness, team-building and defender success rate
- Identified gaps during shift change and improved communications between teams
- Targeted areas for investment – and providing assessment and evaluation

## MAJOR BANK CASE STUDY

**Developing and assessing SOC staff with metrics and range exercises.**


Identify individual & team gaps with data
Mentorship program & training
Individual exercise opportunities
Cyber range team exercises
Reassess and identify new gaps

Framed around a career path for cybersecurity analysts and architects

# V. THE ACTION AGENDA

> **“There is great value in getting experience in stressful situations that are not the real thing; great team building; and a chance to involve less experienced staff.”**
> **– ACSC Member Company**

1 **Create a multi-year training and development plan**

- Focus plan on front-line, blue team and mix in newer staff to get them incident response experience and teambuilding opportunities (consider including interns to aid recruiting).
- Establish clear and measurable objectives aligned to employee development.
- Incorporate diversity and organization engagement goals for senior management and non-technical cyber-support functions.
- Market programs internally to gain participation across the organization.
- Build extra time into exercises for collaboration and evaluation.
- Focus exercises on applications, end-users, and desktops — where the breaches are likely to occur — and less on firewalls.
- Develop plans to include MSSPs and vendors.
- Open up 24/7/365 sandboxes for team and individual testing.

2 **Consider establishing sandboxes with other organizations in order to jointly assess new tools and security innovations.**

3 **But double-down on investments in people and process first.**

> **“Develop a deep team with ongoing assessment by screening job applicants with tests, providing targeted team training and group practice sessions and growing individuals’ skills. And include non-IT stakeholders like legal and communications.”**

4 **And prioritize collaborative exercises to complement internal experiential development and assessments.**

> **“Be holistic...bring in other teams and functions, not just cyber operations.”**

## THE ACSC OPPORTUNITY FOR COLLABORATIVE DEFENSE

### Cyber ranges in action

**PEOPLE**

| Parallel play teams | Joint teams |
|---|---|
| • Individual exercises highlight gaps, track progress and provide peer benchmarks<br>• Shared takeaways across organizations | • Staffs learn from peer organizations<br>• Build peer networks across organizations |

**PROCESS**

- Internal collaboration across technical and business functions in an organization
- External collaboration across private and public sectors

**TECHNOLOGY**

- Assess new technologies and innovative tools in a secure environment through collaborative sandboxes
- Accelerate innovation and reduce costs

# VI. PRESENTERS, COMMENTERS, AND RESOURCES

### RESEARCH PARTNER PRESENTERS

**Paul Winter,** Program Director — SimSpace

**David Berliner,** Director of Product — SimSpace

### CISO CO-CHAIRS

**Patrick Ford,** CISO for Americas Region — Schneider Electric

**Katie Jenkins,** EVP and CISO — Liberty Mutual

**Marc Zissman,** Associate Head, Cyber Security & Information Sciences Division — MIT Lincoln Laboratory

### LEADING PRACTITIONERS

**Jeff Fisher,** Chief Warrant Officer Five — U.S. Department of Defense

**Athie Self,** Vice President, Global Technology Project Manager — JPMorgan Chase & Co.

### EXPERT RESOURCES

**Dan MacDonnell,** Chief Strategy Officer — Randori

**Bill Brown,** CISO & CIO — Abacus Insights

**Matt McHugh,** Director of Information Security, Risk and Compliance — Federal Reserve Bank of Boston

### ADDITIONAL RESOURCE

**Article:** Why Cyber Ranges Are Effective To Train Your Teams

## ABOUT THE ACSC

The Advanced Cyber Security Center (ACSC) is the region's only non-profit, member-driven organization committed to strengthening member cybersecurity defenses and preparing the region's response to large scale cyber threats. The ACSC was established in 2012, as a 501(c)3 organization and was the model for Information Sharing and Analysis Organizations (ISAOs) when Presidential Executive Order 13691 was implemented in 2015. Currently the ACSC has 27 members representing the financial services, healthcare, technology and other sectors, along with leading universities, the Federal Reserve Bank of Boston and the Commonwealth of Massachusetts.