WHITE PAPER

The Case for Cyber Force Platforms

By Jon Oltsik, Enterprise Strategy Group Senior Principal Analyst and Fellow

December 2022

This Enterprise Strategy Group White Paper was commissioned by SimSpace and is distributed under license from TechTarget, Inc.

Contents

Executive Summary

If there's one constant in cybersecurity, it's change. This is true for security teams whether they are called upon to support digital transformation, cloud-native software development, or remote workers. Today, the changes in the threat landscape are driven by growth in ransomware, supply-chain attacks, insidious software vulnerabilities, and state-sponsored cyber adversaries.

In the current environment, it would be an understatement to say that CISOs have a demanding job. These executives are tasked with managing and mitigating cyber risks, protecting critical assets, and detecting and responding to cyber-attacks. In addition, CISOs face a wide variety of audit demands and often struggle to provide appropriate evidence of compliance. Can CISOs keep up? And if so, how?

Research by TechTarget's Enterprise Strategy Group (ESG) shows:

- CISOs often fight an uphill battle. Many organizations approach security with too many tools, a dependency on manual processes and a shortage of labor and skills. What's more, attack surface growth and continuous threats drive cyber risk, leaving organizations open to devastating cyber-attacks. CISOs can't address these problems with tactical adjustments alone. Instead, they need a strategy that addresses business, IT, and security transformation.

- Cyber Force platforms can help level the playing field. New platforms are evolving out of cloud-based cyber ranges and have the potential to help CISOs better address their objectives. How? Continuous security platforms use a cyber range to create a virtual mirror simulation of an organization's IT and security infrastructure, acting as a test site for security team use cases like security baselining, stack optimization, team incident training, staff proficiency advancement, continuous testing, and business/IT initiative support. Therefore, Cyber Force platforms can provide a low-cost/low-overhead foundation for continuous security program improvement.

- Future Cyber Force platforms will introduce CI/CD to security programs. Today's Cyber Force platforms act as a workshop where security teams can test and optimize their people, processes, and technology. Soon, however, market-leading platforms will also act as a development backend for a security-focused continuous integration/continuous delivery (CI/CD) pipeline. Security engineers will develop detection rules, tune controls, and put together security architectures in the platform and then test them using real-world cyber-adversary tactics, techniques, and procedures (TTPs). Once these security defenses are optimized, Cyber Force platforms can allow security professionals to push these changes directly into production environments, improving security efficacy and operational efficiency.

Aside from the CISO and focus on cybersecurity, Cyber Force platforms can also be a business enabler by helping organizations improve brand protection, accelerate IT and regulatory compliance audits, optimize security investments, and help organizations pursue digital transformation initiatives while minimizing associated cyber-risks. These benefits should be especially attractive to CEOs, CFOs, CIOs, and corporate boards.

The CISO Triad

According to Enterprise Strategy Group (ESG) research, 73% of organizations employ a full-time CISO, while another 5% hire a virtual CISO.[1] Just what are these CISOs responsible for? The short answer is that CISOs oversee an organization's cybersecurity program, but security management duties extend beyond this narrow definition. CISO job responsibilities can be summarized using the CISO triad (see Figure 1) and include:

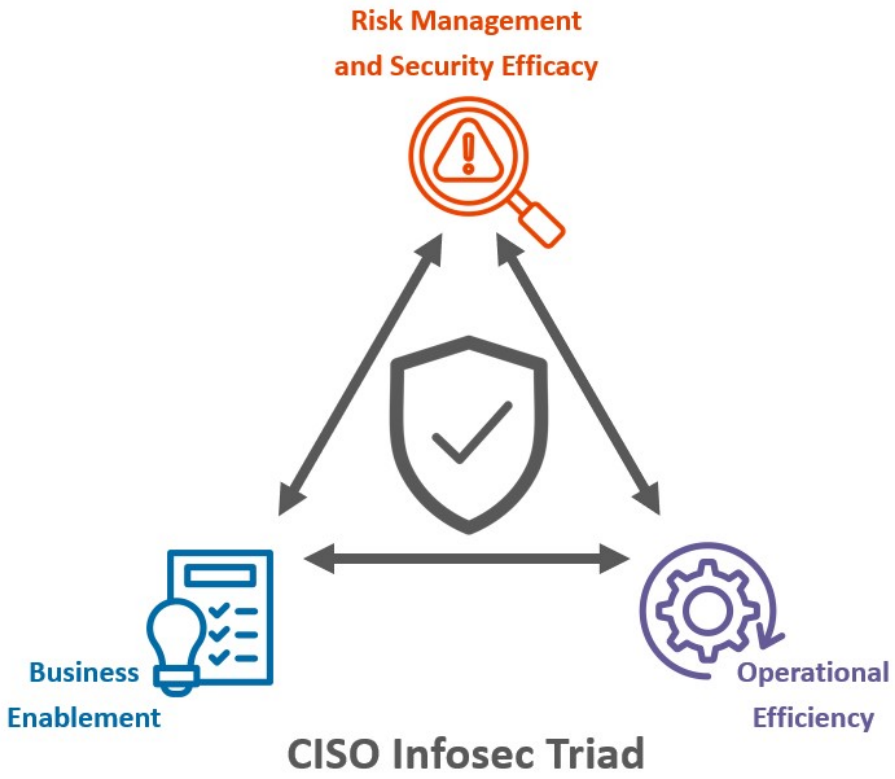
[1] Source: Enterprise Strategy Group Research Report, *The Life and Times of Cybersecurity Professionals 2021*, July 2021.

- Risk management and security efficacy. CISOs supervise the protection of critical business assets, including applications, data, and systems. This includes deploying threat prevention controls (i.e., endpoint security software, network firewalls, email security, etc.), continually monitoring threats and quickly responding when breaches occur. Ensuring security efficacy also involves identifying and mitigating cyber risks and testing security controls and processes to ensure they are working correctly. It also requires reporting capabilities to inform governance boards and compliance oversight.

- Operational efficiency. CISOs must make sure that security is included as a standard operating procedure across the organization. This involves training and maintaining staff, optimizing security processes, and building a program for continuous improvement that can be monitored and measured.

- Business enablement. The saying, "every company is a software company," refers to the fact that organizations are embracing digital applications, IoT devices, and cloud computing to transform business operations. CISOs support digitization by building programs for secure software development, working with engineering teams on cyber resilience and ensuring secure connections with customers, suppliers, and business partners.

Figure 1. CISOs Have Three Primary Responsibilities



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

CISOs Face Relentless Challenges

When asked to rate their CISOs' performance, many cybersecurity professionals offered lukewarm responses. Forty-nine percent said their CISO is only somewhat effective at their job, while 8% indicated their CISO is not very or not at all effective.[2] This lack of confidence may be one reason that the average CISO tenure is between 24 and 36 months.

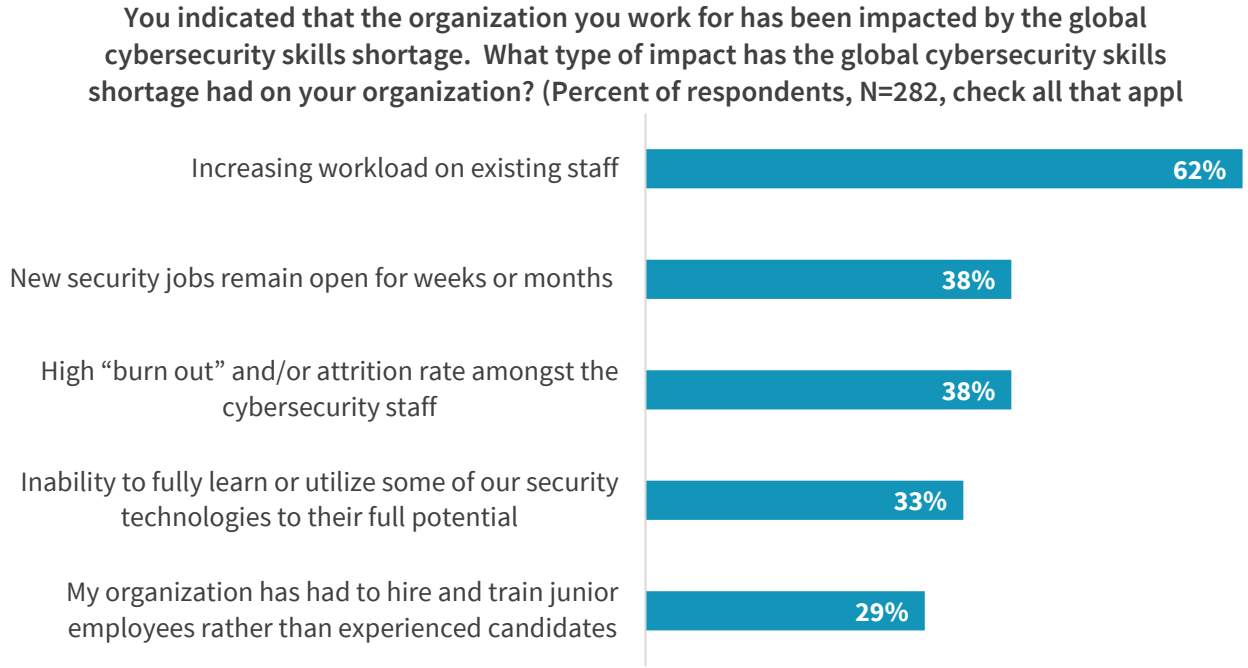
[2] Ibid.

Many CISOs struggle in these areas:

- **Risk management and security efficacy are a game of catch-up.** According to Enterprise Strategy Group (ESG) research, 61% of security professionals agree that their organizations find it difficult to prioritize the security hygiene and posture management actions that have the biggest impact on risk reduction.[3] At many organizations, CISOs and security teams often base important security decisions on best guesses rather than sound data and accurate risk models. Without a convenient and business-relevant way to test the impact of vulnerabilities and to validate the actual effectiveness of their security controls, CISOs aren't sure which vulnerabilities to patch first, if patches are safe, or whether their controls are working until they are under attack.

- **Operational efficiency suffers across people, processes, and technologies.** After years of research, ESG concludes that many security departments face three common issues: 1) They manage security using too many disconnected point tools. 2) They rely on manual processes. 3) They tend to be understaffed and often lack advanced skills in one or more key areas. The ramifications of the talent shortage are especially troubling. According to research from ESG and the Information Systems Security Association (ISSA), 57% of organizations say they have been impacted by the global cybersecurity skills shortage. The gap results in increasing workloads for security teams, open job requisitions, high burnout and attrition rates, and an inability to fully learn or utilize security technologies (see Figure 2).[4]

Figure 2. Top Five Implications of the Cybersecurity Skills Shortage



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

- **Business enablement is difficult when there is a disconnect between the CISO and executives.** Industry leaders agree that cybersecurity should be integrated into business planning and processes, but 28% of organizations still view cybersecurity entirely as a technology area. Another 41% view cybersecurity mostly as a technology area but with some emphasis on the business.[5] While business executives own some of the blame here, CISOs are also responsible

[3] Source: Enterprise Strategy Group Research Report, *Security Hygiene and Posture Management*, January 2022.
[4] Source: Enterprise Strategy Group Research Report, *The Life and Times of Cybersecurity Professionals 2021 Volume V*, July 2021.
[5] Source: Enterprise Strategy Group Research Report, *Cybersecurity in the C-Suite and Boardroom*, February 2021.

for this disconnect. Many fail to communicate with executives and boards in business terms, relying instead on technology jargon around open vulnerabilities, indicators of compromise (IoCs), and mean time to detection or response (MTTD/MTTR). To bridge the gap, business and security leaders need common models and a shared lexicon to improve communication.

Even when CISOs believe they are managing the triad effectively, they often lack real data or metrics to understand their security posture. As a result, they may lack confidence in the abilities of their security staff, technology stack, or the entire enterprise security program.

Cyber Force Platforms Can Help Bridge the Gap

As described above, there is often a disconnect between security objectives and results, and it can be difficult to address short-term gaps while mapping out a longer-term strategy. So, what is the best way forward?

Enterprise Strategy Group (ESG) believes Cyber Force platforms can guide better decision making for CISOs, as Cyber Force offers a controlled, interactive technology environment where cybersecurity professionals can train and advance their skills using the same kind of equipment they have on the job. A range can be used to simulate attacks on a virtual version of an organization's technology and security infrastructure, enabling organizations to validate security controls and processes.

In the past, cyber ranges were expensive to build and maintain, which limited their use to military, intelligence agencies, and large well-resourced organizations. Fortunately, this is no longer the case. With the proliferation and maturation of public cloud computing, cyber ranges are now widely available.

With public cloud scale and tooling as a foundation, some cyber range providers, like SimSpace, have transformed their offerings into fully functional Cyber Force platforms. With the ability to precisely simulate an organization's hybrid IT infrastructure and security controls, Cyber Force platforms go far beyond training alone, offering use cases like:

1. Security baselining. Before proceeding with security planning, CISOs must have an accurate understanding of their security posture. Cyber risk management platforms can help with this type of baselining by assessing all security controls, processes, and personnel. This highlights gaps and cyber risks, enabling CISOs to prioritize investments that safeguard business-critical assets. They can also track ongoing projects and initiatives, gaining evidence for compliance and identifying areas where their programs lag.

2. Stack optimization. As previously mentioned, many organizations run security with an army of disconnected point tools, which makes it difficult to tune their tech-stacks and identify redundancies. Using a Cyber Force platform, CISOs and their SOC leaders can assess individual tools as well as the whole stack using manual or automated tests within a simulated version of their environment. By doing so, InfoSec teams can run test cases for vendor integration and consolidation and get a clearer picture of how their tools function in concert. Security engineers can also use simulation to develop, test, and fine-tune detection using Yara and Sigma rules. With a secure, high-fidelity test bed, organizations can evaluate new technologies, qualify vendors, and determine final candidates for product bakeoffs, pilots, and production rollouts.

3. Staff proficiency and improvement. ESG research indicates that 70% of cybersecurity professionals say it is extremely difficult or somewhat difficult to hire and recruit cybersecurity staff,[6] so it's unlikely that CISOs can hire their way out of their current staffing and skills deficits. Accordingly, organizations must do all they can to retain

[6] Source: Enterprise Strategy Group Research Report, *The rise of cloud-based security analytics and operations technologies*, December 2019.

the talent they have and support their careers. The best way to keep their best people is to give those individuals support in bolstering their own skills and productivity; companies improve their talent retention by 58% when they invest in training.[7] Recent ESG/ISSA research revealed that 39% of security professionals believe their organizations could address the global cybersecurity skills shortage by increasing their commitment to cybersecurity training.[8] A Cyber Force platform can help here in several ways. Security teams can take advantage of basic cyber range capabilities for hands-on team training and tabletop exercises that use cyber-adversary TTPs against an emulated version of the organization's IT/security infrastructure. Based on the results of these tests, organizations can reassess skills development needs, mentoring programs, and workflows.

4. Continuous testing. Nearly half (47%) of security professionals believe that penetration testing and red team exercises are a risk management best practice, but most organizations can only conduct security testing periodically.[9] With the right platform, security teams can increase security testing frequency across security controls, processes, and personnel without disrupting day-to-day operations. This can be especially useful for operationalizing the MITRE ATT&CK framework, as a Cyber Force platform can help determine data source coverage and gaps, assess individual security control efficacy, and test detection rules against known adversary groups and campaigns. Data gathered through these tests can also be used as evidence for regulatory compliance audits.

5. Business and IT initiative support. To improve alignment between cybersecurity and the business, 33% of business, IT, and security professionals believe their organizations should involve the security team earlier in business planning, major initiatives, and software development.[10] A Cyber Force platform can help by emulating new programs, aligning deployments with risk models, and building the right security controls into all business processes. For example, an organization can use a range to emulate a Zero Trust infrastructure, test it against known attack campaigns, discover vulnerabilities, and then apply the right countermeasures to maximize protection. This type of business and cyber risk modeling can also help organizations work with cyber insurance providers to optimize premiums and coverage.

Cyber Force Platforms Will Anchor Security CI/CD

In the future, Cyber Force platforms will go beyond these use cases, allowing organizations to shift left with security planning. How? Security teams will make all security changes in the platform, enabling them to evaluate controls, test defenses, and fine-tune controls. They can also use manual or automated testing tools to test the efficacy of these changes against adversary TTPs and adjust them accordingly. Once the simulated environment meets all quality and efficacy milestones, security teams will be able to push changes directly from the range into their production systems. Like DevOps automation tools, the cyber range will ultimately serve as a foundation for a continuous integration and delivery pipeline, focused on constant cybersecurity improvement.

The SimSpace Cyber Force Platform Provides Military-grade Cyber Ranges

While the Cyber Force platform concept may be unfamiliar, SimSpace is well on its way to delivering on these capabilities. SimSpace markets itself as a "Cyber Force Platform," supporting an ecosystem of hundreds of security products, training

[7] Source: Enterprise Strategy Group Survey Results, *The Life and Times of Cybersecurity Professionals 2021*, June 2021.
[8] Source: Enterprise Strategy Group Research Report, *The Life and Times of Cybersecurity Professionals 2021 Volume V*, July 2021.
[9] Source: Enterprise Strategy Group Research Report, *Security Hygiene and Posture Management*, January 2022.
[10] Source: Enterprise Strategy Group Research Report, *Cybersecurity in the C-Suite and Boardroom*, February 2021.

content from leading security education providers, and certification frameworks to ensure an organization's teams, technology, and processes are always ready and optimally tuned.

SimSpace provides a range-as-a-service model, delivered from the public cloud. This simplifies deployment and customization, enabling organizations to achieve benefits quickly. SimSpace aligns with the use cases described above through the following capabilities:

- SimSpace Military-grade Cyber Range. This is the engine that makes everything work and provides the foundation for SimSpace's advanced capabilities. The SimSpace military-grade cyber range is high-fidelity and provides users with a customizable, simulated environment that delivers a safe and secure platform for a host of activities. Advanced user emulation creates a dynamic context for security operators to explore, while APT-based and AI/ML-enabled automated attacks put those operators and the organization's security stack to the test.

- Elite cyber training. Elite special forces-level cyber training helps security leaders manage individual growth and team performance by providing end-to-end range-based learning opportunities, such as live-action assessments, mission rehearsals, and individual or team exercises, each with automated scoring and clear performance metrics. SOC managers can guide their teams to greater performance, while CISOs gain visibility into the readiness of their organizations and can retain top performers.

- Stack optimization. Stack optimization provides a unique, automated, data-driven tool to test the efficacy and useability of a full stack of security products. This can provide customers with the ability to streamline their defense in depth, mitigating costs while gaining effectiveness.

Together, these capabilities give SimSpace customers the ability to gain visibility into their cyber risk and readiness. They can run real-world scenarios, assess business, compliance, and even cyber insurance risk profiles, while gaining insights that can give their boards a better ability to understand the maturity of their cyber operation. Tracking event performance over time, SimSpace customers have seen meaningful improvements in attacks defended, through increased tool efficacy, improved processes, and greater talent.

SimSpace customers typically start by using the cloud-based cyber range for training and testing purposes. While this is a great place to start, we believe that organizations can gain additional benefits when they use SimSpace to shift left. This means deploying and testing security in a virtual environment, optimizing processes and controls, and then automatically pushing these changes to their production environment. With this use of the SimSpace platform, CISOs can establish the right foundation to address all aspects of the CISO triad.

The Bigger Truth

CISOs walk a tightrope, balancing business, technology, and risk factors along the way. However, all these areas are in a state of constant change. Businesses are growing more remote and digitized. Technology infrastructure is moving to the cloud and network edge while applications use cloud-native services like containers and serverless functions. And cyber risks like ransomware, supply chain attacks, and critical vulnerabilities remain pervasive.

Managing all these changes is difficult and likely accounts for the fact that many CISOs last just two or three years at each job. What would help? A virtual laboratory where organizations could plot out changing business and technology conditions, add security controls, observe the results, and then adjust defenses to optimize protection. It would also be valuable if such a laboratory could be used to test process efficiency and staff proficiency and then help improve these areas.

A Cyber Force platform has the potential to deliver all these benefits. We expect that leading security platforms will go further, creating a CI/CD pipeline as a cybersecurity foundation. With the right range deployment, security testing, detection rules development, and process improvement can be conducted in a virtual environment, fine-tuned, and optimized before being pushed to production. This cycle will then be used for continuous improvement. As this happens, Cyber Force platforms will become a foundational requirement for enterprise security programs.

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com

contact@esg-global.com

508.482.0188