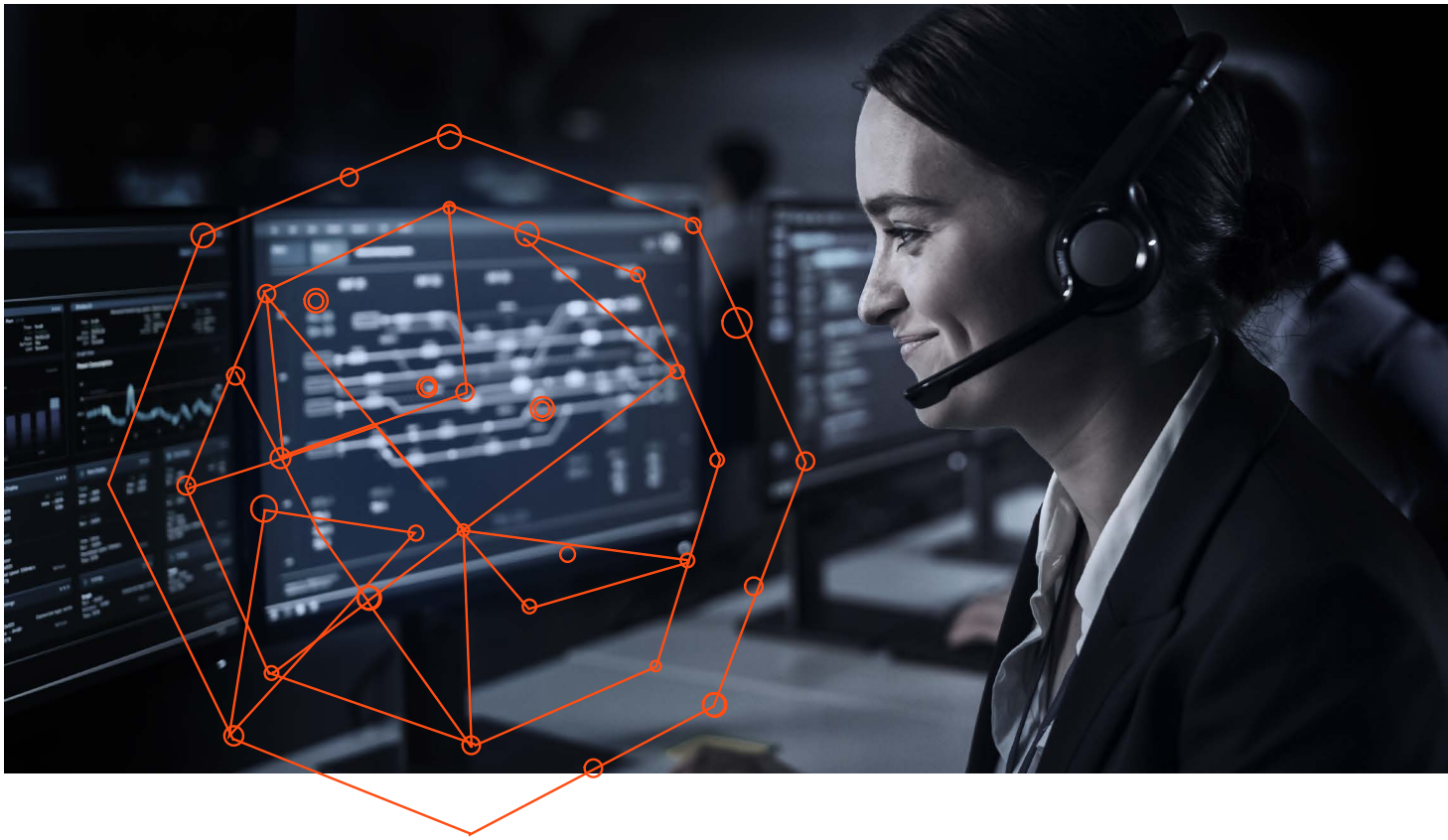
whitepaper



SimSpace 101

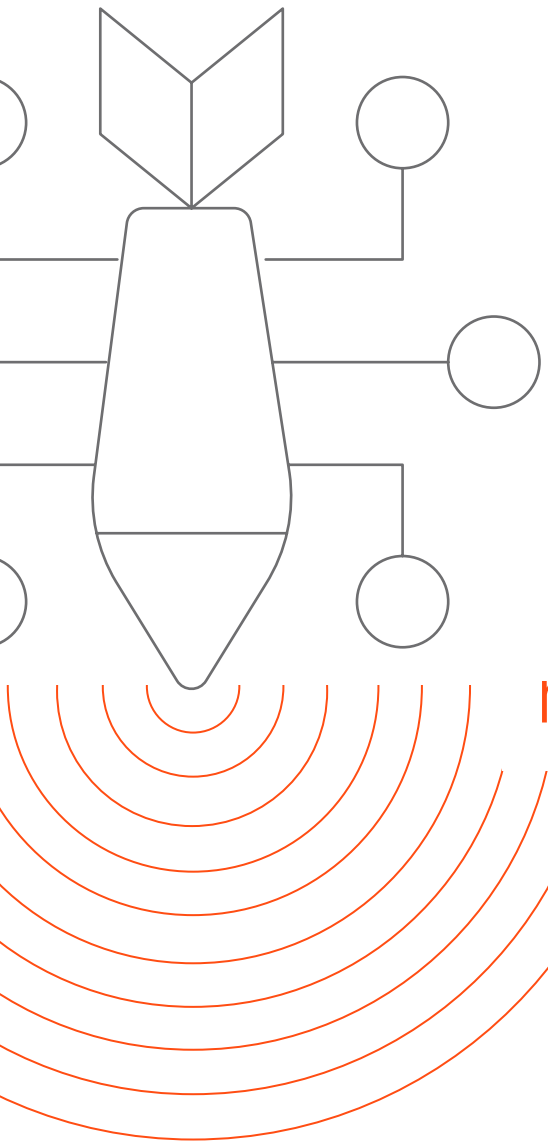
Four Reasons to Use a Cyber Range

You've invested in the tools and personnel to get the job done – how do you know what's working?

SIMSPACE
SECURE WITH CONFIDENCE

Contents

Introduction



In July 2021, a major IT and security management provider announced they had suffered a supply-chain attack. The breach was especially devastating because the company sells software to multiple managed service providers (MSPs). This meant the impact was far-reaching, infecting clients as well as hundreds of MSPs and their customers — primarily small and medium-sized businesses. Victims could choose to pay the ransom ($45,000 for individual firms and $5 million for MSPs) or ignore the threat and try and rebuild compromised assets through backups. Unfortunately, this was not the only major ransomware event in 2021, as there were 2,690 reported ransomware attacks in 2021 compared to 1,389 in 2020, a 92.7% increase year over year.[1]

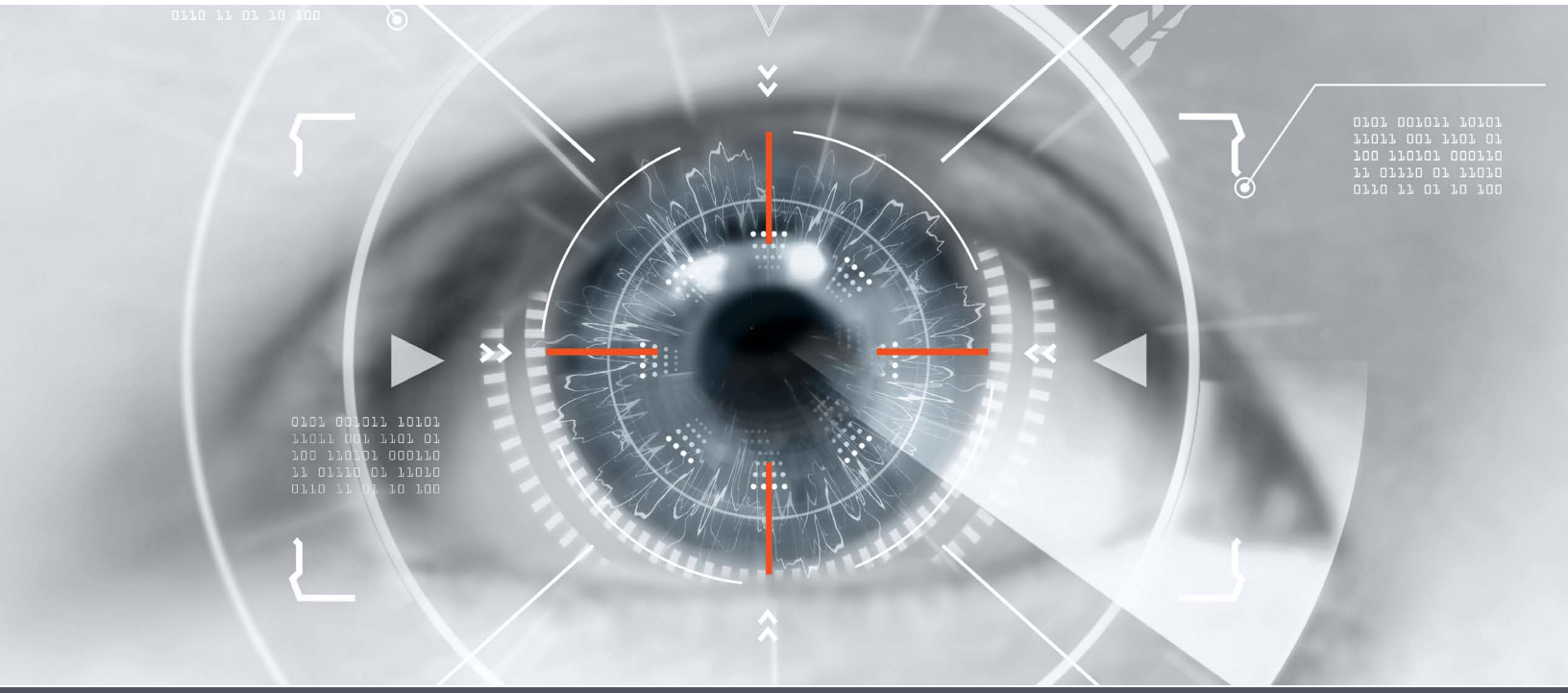
ransomware events

[1]NCC Group Annual Threat Monitor 2021

With the massive spike in ransomware and other cyberattacks, preparation is key. But how exactly can an organization prepare for such a wide range of incidents across an ever-growing attack surface? The best way is to have your security team practice defending against actual attacks using cyber range training simulations – without risking or impacting production environments. Cyber ranges also allow organizations to assess their cyber defense tools and their team's ability to scan incoming and outgoing messages for malware, block malicious IP traffic, prevent spam, and thwart unauthorized software from entering and spreading throughout the network.

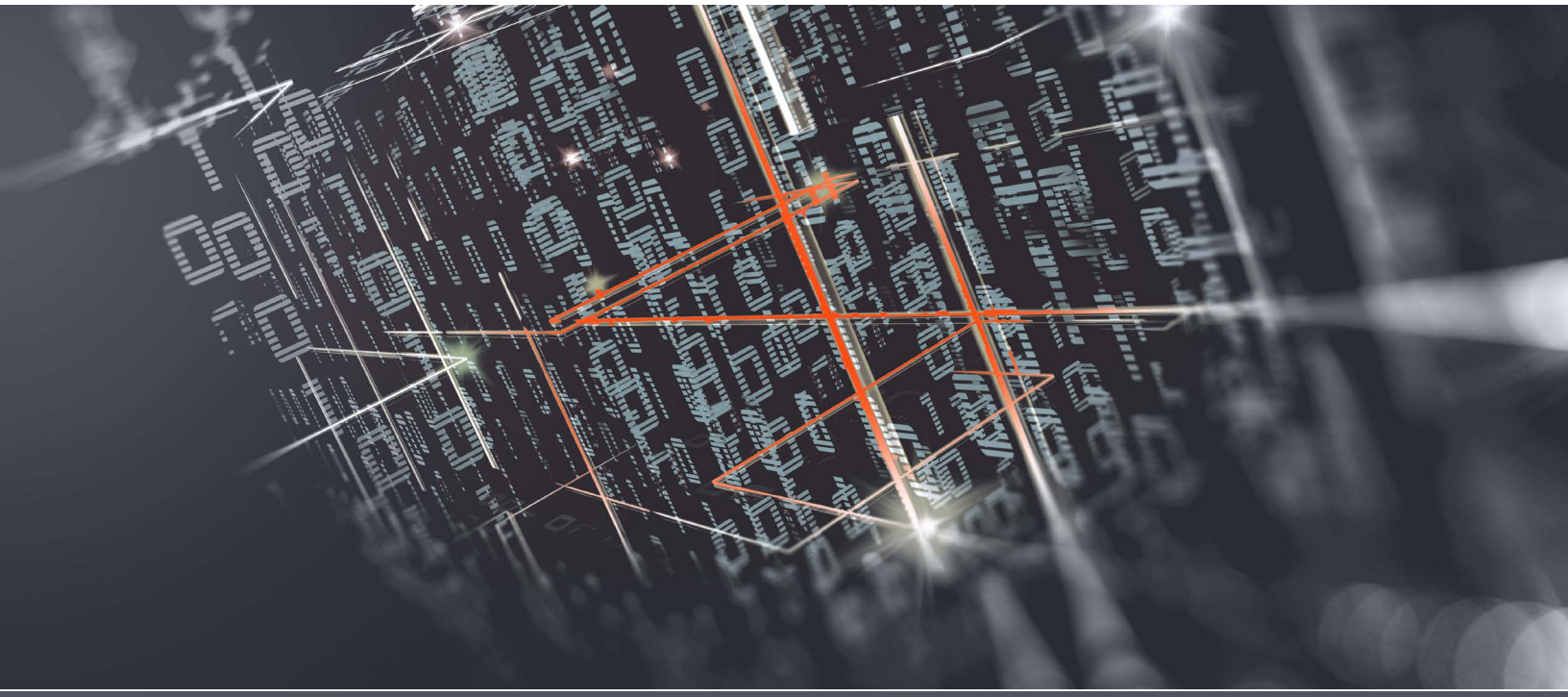
Organizations can also determine if their backups and existing data recovery tools and procedures will be effective in the event of an attack. Our experience working with security professionals across the globe has shown us that teams using a cyber range platform for realistic cyber-crisis training are better able to detect and respond to advanced threats. They also have a much better understanding of which tools work and which ones don't.

Practice defending against actual attacks using cyber range training simulations – without risking or impacting production environments.



What is a Cyber Range?

A cyber range is a realistic, safe, contained and interactive environment where cybersecurity professionals learn how to detect and respond to cyberattacks with the same tools they use on the job. The range simulates real-world attacks on IT infrastructure, networks, software platforms and applications. The right platform will also provide a method to measure progress as employees complete training. Through hands-on experience and technology optimization, a cyber range helps impart confidence in security personnel, tools and processes.



Why use a cyber range?

1

A cyber range **reduces complexity**

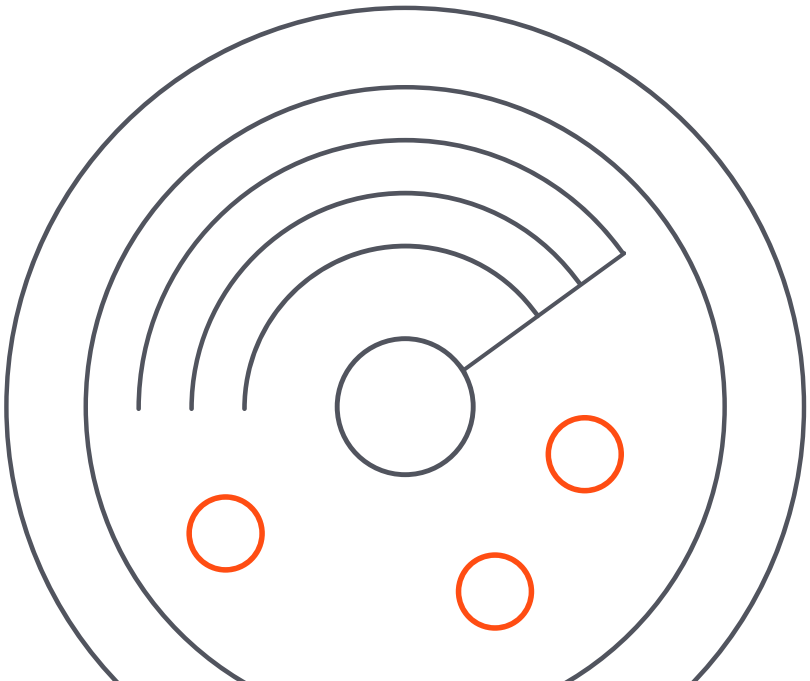
Organizations of all sizes are now aware of their growing risk exposure due to increased connectivity and technological progress. Many are responding by purchasing more cybersecurity tools to boost their defenses as additional cyber threats and attacks emerge, but they often reach a point of diminishing returns.

37%

of organizations self-reported having too many security tools to achieve cyber resilience

On average, enterprises use 45 cybersecurity tools on their networks. However, bolting on additional tools is not always the best defense against cyber threats and often adds unnecessary complexity. An IBM survey found that after a certain threshold, the number of security tools an organization was using actually harmed its ability to detect and respond to an attack. Organizations using more than 50 security tools ranked themselves 8% lower in their ability to detect and 7% lower in their ability to respond to an attack than respondents using fewer tools. Additionally, 37% of organizations self-reported having too many security tools to achieve cyber resilience.[2] With each additional tool that's added, the security operations center (SOC) is bombarded with new alerts. The added signal noise often results in missed alerts, longer response times, and SOC staff burnout and turnover.

A cyber range helps organizations reduce security stack complexity. The tool also enables detection engineering, so practitioners can make sure their cybersecurity tools effectively identify threats relevant to their business, processes or industry. Further, practitioners can use a cyber range to reduce the overall number of cybersecurity tools being used. By evaluating the security stack in a high-fidelity simulation, organizations can use objective data to identify redundancies. And fewer tools means less complexity, because fewer people are needed to operate them.



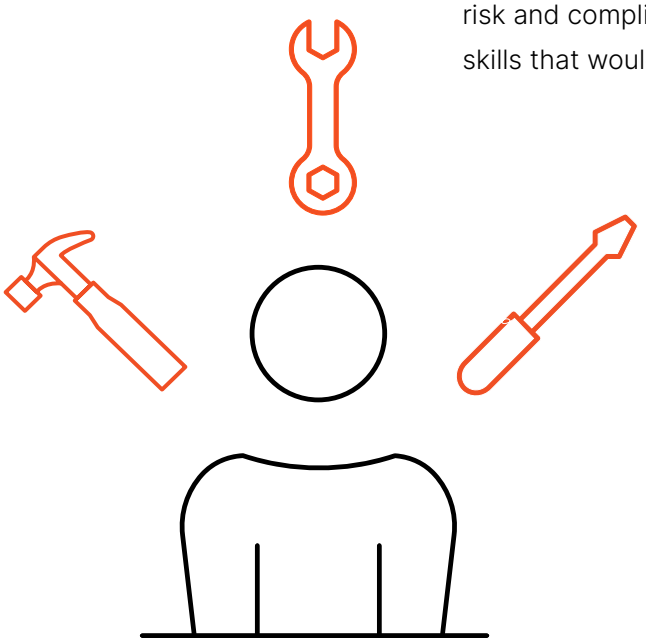
[2]IBM Cyber Resilient Organization Study

2 A cyber range **helps mitigate the cybersecurity staffing crisis**

To build a successful cybersecurity program, organizations must hire and develop the right people.

As threats and cyber risk management technologies evolve, organizations increasingly need skilled talent to operate these tools. At the end of 2021, there was a security workforce gap of 377,000 jobs in the U.S. and 2.7 million globally.[3] Although there is an ongoing, urgent need for cybersecurity professionals, these individuals do exist, and the industry can close the talent gap with the correct training programs and HR practices. This involves a two-pronged strategy — recruiting diverse candidates and retaining top talent.

To build a successful cybersecurity program, organizations must hire and develop the right people. This means going beyond conventional hiring practices to find diverse and non-traditional candidates when filling cybersecurity roles. For instance, women, who are generally more educated, make up less than a quarter (24%) of the cybersecurity workforce — up from 11% in 2017.[4] In addition to building more inclusive hiring practices, it's important to tap into new talent pools. Many candidates with backgrounds in IT have the skills to be successful in cybersecurity. And even those in disparate roles, such as accounting, risk and compliance, and finance, have transferable skills that would serve them in a cybersecurity career.



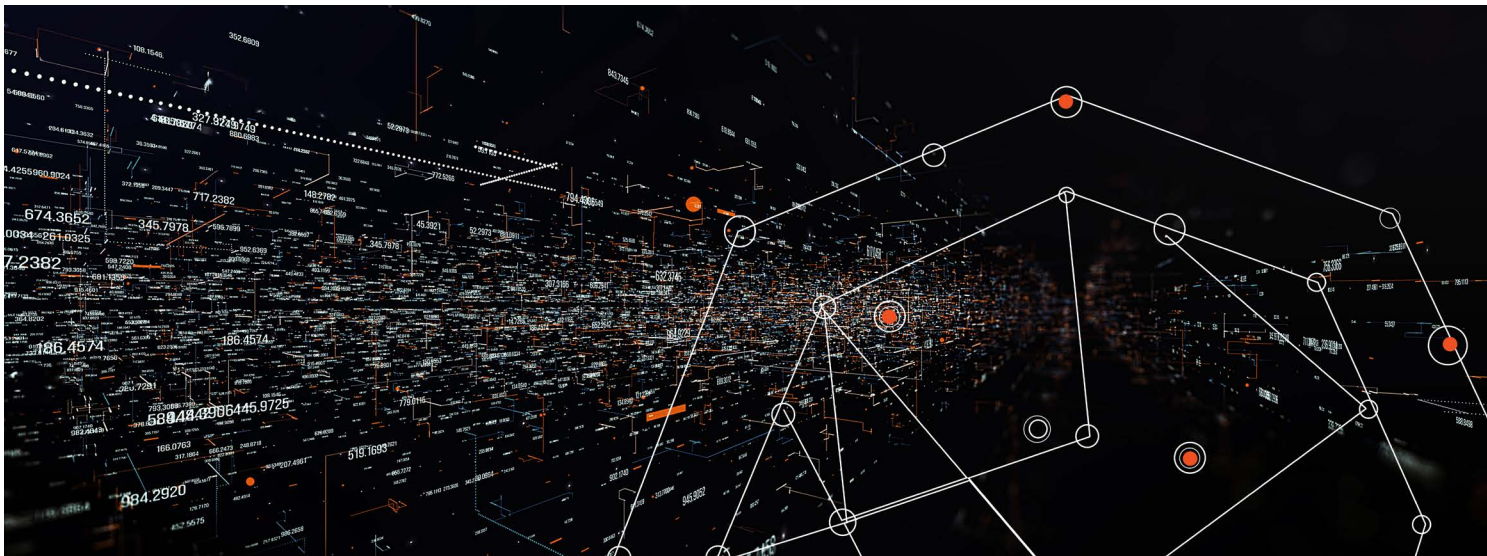
[3](ISC)2 Cybersecurity Workforce Study, 2021
[4]An (ISC)2 Cybersecurity Workforce Report: Women in Cybersecurity

Retention is another important factor in managing cybersecurity staffing shortages. In the aftermath of the COVID-19 pandemic, 51% of cybersecurity professionals report feeling burned out,[5] and a startling 54% are contemplating leaving their job.[6] In addition to the steep monetary cost of backfilling a role, firms lose that employee's job-specific knowledge, which can take months of training to replace.

A cyber range also helps mitigate cybersecurity staffing shortages by boosting training programs. Organizations can provide additional training to anyone with a passion for learning about cybersecurity, which brings in diverse talent pools and career changers. Additionally, improving training drives retention, because employees feel like their company is investing in them and empowering them to do their jobs. Investing in training also drives internal growth. With team training specifically, individuals feel more connected to and confident in their overall team.

3 A cyber range **enables companies to defend against emerging threats**

It's easier to practice defending against well-known threats and vulnerabilities, but often organizations are compromised via new threats and vulnerabilities. Businesses that wish to remain competitive must deploy newer technology, and doing so exposes them to emerging threats. Employees can learn to defend against these evolving attack techniques by training on a cyber range that features continually-updated threat libraries. With dynamic training content, organizations can test out the most damaging cyberattacks in a safe, high-fidelity replica of their production environment, providing hands-on experience without any enduring effects on the network.



One of the many emerging attacks SimSpace helps companies defend against are ***data manipulation attacks*** — a growing trend. These attacks alter or delete data for long-term financial gain and tarnish a victim organization's reputation. They are especially prevalent in the financial industry — for example, wire fraud or credit card micropayments. The confounding feature of a data manipulation attack is the difficulty in determining the extent of the damage or exactly how threat actors manipulated the data. Cyber ranges allow your organization to test technical and policy defenses against these attacks. First, have a policy in place as well as education around how critical data is sent through secure channels. Then, evaluate your technical defenses — such as encryption and multifactor authentication — by simulating attack scenarios in a range.

One of the many emerging attacks cyber ranges help companies defend against are data manipulation attacks — a growing trend.

Other examples of emerging threats that a range can help mitigate include insider threats and advanced persistent threats (APTs). Insider threats involve privileged users abusing their access to company data and systems. With an advanced cyber range that includes realistic virtual users, you can simulate insider threat scenarios, such as abuse of user credentials and unauthorized access requests. An APT is generally classified as a long-term presence on a government or large enterprise network to mine sensitive data. These complex attacks can be challenging to detect and mitigate, but a cyber range allows teams to replicate these attacks in a safe training environment.

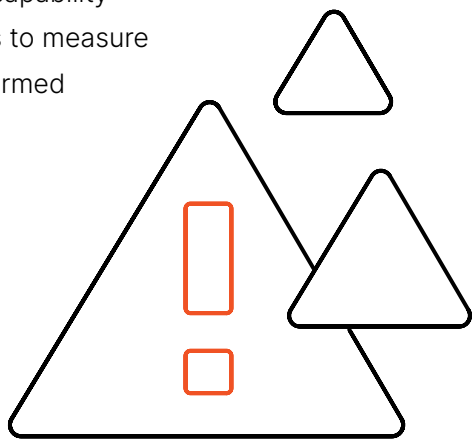
4 A cyber range **helps prove ROI to stakeholders**

There is a quantifiable reputational and financial impact when a company suffers a cyberattack, such as a data breach. Immediately after announcing a breach, firms experience a 5% stock price decline on average.[7] Customer trust often takes a hit as well. A Forbes and IBM study found that 46% of organizations experienced damage to their reputations after suffering a data breach.[8] Other impacts include service and logistical disruptions, data loss and regulatory fines.

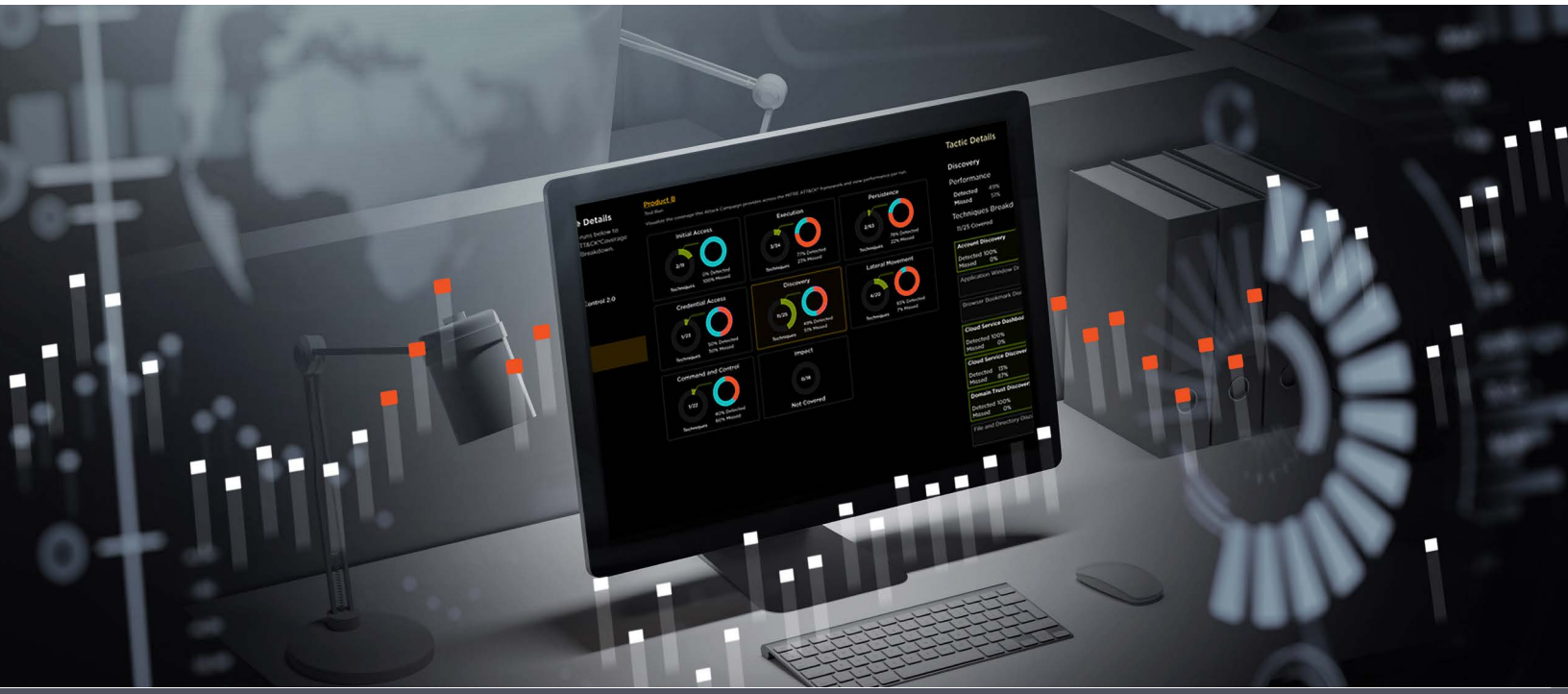
When working correctly, cybersecurity investments prevent loss. But unfortunately, it can be hard to measure the return on these investments without experiencing the consequences of an actual incident. By leveraging a platform that provides in-depth strategic exercises and performance metrics, companies can evaluate the response of their people, processes and technology to a real-world cyberattack — without real-world consequences. This capability makes it easier for management, boards and executives to measure and augment their cyber readiness by making more informed investments.

46%

of organizations experienced damage to their reputations after suffering a data breach



[7] Centrify/Ponemon Data Breach Impact Study, 2017
[8] Forbes/IBM Fallout: The Reputational Impact of IT Risk



How SimSpace helps

The world's most advanced commercial cyber range

The world's most advanced commercial cyber range powers the SimSpace Cyber Risk Management Platform, providing everything needed to keep your people, processes and technology operating at peak performance. With hyper-realistic simulated environments, you can see how your defense mechanisms respond to actual cyberattacks. That means you can optimize and consolidate your tech stack, build better training programs, perform more effective candidate evaluations and leverage actionable insights to make more informed business decisions.

Ready to learn more about how SimSpace can help you build confidence in your cybersecurity posture? Click here to request a demo.

simspace.com info@simspace.com

SIMSPACE