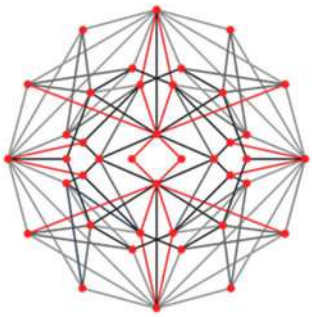

RANGEFORCE

Cybersecurity Training: Stop Calculating ROI and Start Calculating Savings

Making the business case for RangeForce Cyber Skills Training

By David Koff

Abstract

Security teams today spend hundreds of thousands of dollars on training their security teams. They struggle to find qualified staff to fill open security roles, and incur the cost of bad hires. Some companies additionally spend hundreds of thousands of dollars to build or buy a cyber range service to create a more effective training environment. All told, these numbers quickly reach seven figures. This paper explores how the RangeForce CyberSkills Training Platform can cut those costs by an amazing 75%.

Dec 2019

RANGEFORCE

Introduction: Cybersecurity Training: Stop Calculating ROI and Start Calculating Savings

The day-to-day pressures of being a CISO are enormous and extend to far more than matters of incident response time. There are pressures to report performance to management, pressures of creating and maintaining budgets, pressures to do more with less, and at a time when the scope and number of cyber incidents are increasing, the pressure to find qualified candidates to fill an unusually large number of unfilled security positions.

> *"It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it."*
>
> Stephane Nappo

Where does cybersecurity training fit into those ever-competing pressures? And how can a company's C-suite reliably believe in what their CISO is telling them? Never mind that this Forrester Research white paper suggests a 115% ROI for cybersecurity training. And never mind that this second Forrester paper suggests a 336% ROI for the same.

Numbers can be misleading, trends can be smoothed over with charts and graphs, and details can be lost in translation at a time when training is so incredibly important. Leaders and decision-makers won't make a business case if all products make the same claims. Instead, today's CISOs need data that demonstrates how the team is actually doing and that what is already being spent can be made better.

What's needed is clear, simple math that any CISO can present to upper management. Let's dive in and explore the three core ways that can help CISOs make a business case, through cost savings, for cybersecurity training using RangeForce.

For our examples, we'll use the scenario of hiring or training ten employees over one year.

Category #1: Reducing the Costs of Training

Companies already spend money on cybersecurity training. A lot of it, as it turns out. Most of the courses offered at the SANS Institute — one of the premier cybersecurity training firms in the world — run between $6,000 - $7,000. That's per module/class. That means that a company with ten security staffers who require training or certification in only five classes can spend over $350,000 annually on that training.

These astronomical costs and travel restrictions are why some companies have turned to online training. But in many cases, that approach has financial limitations as well. The cost of online classes, on-site hardware setup, the restriction of access to classes, the licensing costs of just

one class, and the creation of one set of labs per person is prohibitively expensive. If each user takes five online classes annually, the cost for SANS courses run as much as $325,000 annually for the same ten users. It should be noted that both online and classroom training is considered complete at the end of the class. There is no continued or ongoing training environment where the cyber pro can practice and refresh their new skills.

By comparison, RangeForce offers its entire on-demand training platform — including 90+ modules and growing — as a single package available for all security team members at any time for a flat cost of $2000 per user per year. There's no travel or lodging required and no hardware or set up costs as the courses are delivered through a cloud-based virtual service. There's also very little lost time at work: employees can train for an hour a day and gain relevant experience from the comfort of their desk, rather than losing five days for SANS training.

The savings here are significant. A team of 10 security staff will cost just $20,000 per year with a per-module price of only $22 per module/per user (which is included in the $2000 annual license). More importantly, CISOs can rest easy knowing that their cybersecurity team will continue to receive hands-on training with a company that's always adding new modules and training (as many as four new modules per week all of which is included in the annual fee), based on the most-recently occurring cyber-attacks.

With access to all training modules for all users, RangeForce also allows your existing teams to become cross-trained: that way, your current staff gets better at handling other kinds of threats and expands their abilities.

By providing its platform in the way it does, RangeForce can offer today's CISO real-world savings of over $330,000 annually, all while preserving each security team member's daily at-work incident-response duties and performance. And $330K is a figure every CFO will notice.

Category #2: Eliminating the Need and Cost of Creating a Cyber Range

Setting up a proper cyber range is difficult, yet some companies choose to build their own cyber range in a well-meaning effort to provide a more realistic training and "safe" pen-test environment. This is a worthy but often costly and time-consuming endeavor. The complexity of the hardware and software procured, the expertise of the individuals who are setting up the environment, and the time required to prepare the range can run into the hundreds of thousands of dollars in purchases and cost untold labor-hours. Organizations can spend months setting up their own cyber range at the cost of $500,000. But that's just the price for setting up a range: it doesn't take into consideration the additional costs of planning and executing various exercises to operate the range. Those can run $50,000 to $100,000 each, and there are many cases of companies creating cyber ranges and then never actually using them.

As a result of the time and cost required, some companies choose to implement a cyber range service from companies like Raytheon and Cisco. But those costs are also quite high. Cisco, for example, offers a 5-day exercise on their cyber range for up to 12 people for $51,500.99

By comparison, RangeForce has built a scalable cyber range into its training platform, which is designed to execute advanced cyberattack simulations. Notably, their platform includes RangeForce's own virtual red teams, so that both the setup and operating costs are baked into the product. CISOs that rely on RangeForce can offer an amazing real-world savings of up to $500,000 in cyber range setup, training, operations, and staffing costs.

Category #3: Reducing the Costs of Hiring and Retaining Staff

Cybersecurity jobs are in high demand. In fact, there are too many security roles to fill and not enough qualified candidates to fill them. Assuming that you've acquired the budget to hire additional security staff and then spent money on agencies to spotlight possible matches, CISOs then need to consider two crucial elements of the hiring process: weeding out bad hires before jobs are offered and onboarding new staff that have been vetted.

Weeding Out Bad Hires: RangeForce provides an easy way to vet candidates before they're hired. Want to find out if a promising candidate really understands XML, SQL-injection, Botnets, or PHP? Invite them to log into RangeForce and test their skills to determine if their resume and skills actually match. RangeForce will then provide a customized report of these assessment results. The average salary for a Security Operations Center Analyst is around $80,000, according to Glassdoor. The agency costs for finding a candidate runs another $16,000, or 20% of the base salary. Finally, the onboarding costs for a new employee can run as much as $6000.

RangeForce offers talent acquisition and hiring managers a special "hiring assessment license" modeled on "the number of assessments" needed annually. On average, a company assesses five candidates per opening and has ten openings to fill; then, they would assess 50 candidates. A RangeForce pack of 50 assessments is $5000.

If it takes six months to determine that a newly-hired candidate is not going to work out, then the cost of that lousy hire equals around $62,000. Eliminating just one bad hire a year using RangeForce saves that mistake from occurring with an investment of just $5000 and a savings of $57,000. If you eliminate ten candidates over the year, your savings are $570,000.

Bringing New Staff up to speed (time to value): By some estimates, it takes up to eight months to fully train a new SOC staffer. If an annual salary is $80,000, those eight months equal an investment of over $53,000 in salary cost to bring one new hire up to speed. Hire ten new employees, and the cost grows to $530,000. Using RangeForce dramatically reduces the time it takes to train, cross-train, and onboard new hires because of how it programmatically tracks training through its modular training design.

Managers, CISOs, and C-suite executives can easily see reports of progress for all new security hires and watch as mastery of skills are taught, tested, and recorded on a regular basis. If RangeForce can reduce onboarding time by just 25% - from eight months to six months - that saves $11,000 in unproductive salary cost per new hire or $110,000 per ten new hires (RangeForce customers report seeing time to value for employees decrease by as much as 30%).

How Much is it Possible to Save?

For a company that's looking to hire ten new security staff, RangeForce can save up to $330,000 in training costs annually. For a company considering building their own cyber range, RangeForce can save the company up to $550,000 in cyber range costs. For companies looking to fill ten open security roles, RangeForce can save a CISO $57,000 every time a potential bad hire is eliminated or $570,000 if ten potential bad hires are eliminated. Finally, by increasing the efficiency of getting new hires up to speed, RangeForce can reduce lost salary costs by $11,000 per new hire or $110,000 for a staff of ten.

Table 1: Cost Comparison

	Traditional/Build	RangeForce	Savings
Training (1)	$350,000	$20,000	$330,000
Cyber Range (2)	$550,000	Included	$550,000
Bad Hire Cost (3)	$620,000	$5000	$570,000
Employee Time to Value (4)	$530,000	$420,000	$110,000

Notes:

1) Annual estimated training costs for a team of ten
2) Estimated cost of building a cyber range and operating it for one year
3) Estimated costs of eliminating ten bad hires versus a 50-pack RangeForce assessment license
4) Estimated time to value savings based only on salary costs of ten new hires - training with and without RangeForce.

Taken all together, these use cases total a potential a $1,560,000 in savings. If you exclude the cyber range and just focus on the employee costs, the total is $1,010,000 annually. Let the rest of the industry talk about ROI. We can have that conversation later. But first, let's talk about the money you'll potentially save just by choosing RangeForce as your on-demand cybersecurity training platform.

About RangeForce

RangeForce delivers the industries only integrated cybersecurity simulation and skills analysis platform that combines a virtual cyber range with hands-on advanced cyber defense training. Security and I.T. professionals from governments, financial services, universities, and hi-tech companies use RangeForce to qualify their new-hires, training up there DevOps, IT and Security Staff, and run CyberSiege simulations of the latest attack methods to evaluate team skills and detection and response processes. Only RangeForce can accurately show you where your skills gaps exist, fill those gaps through on-demand training, and accurately report on the entire process.