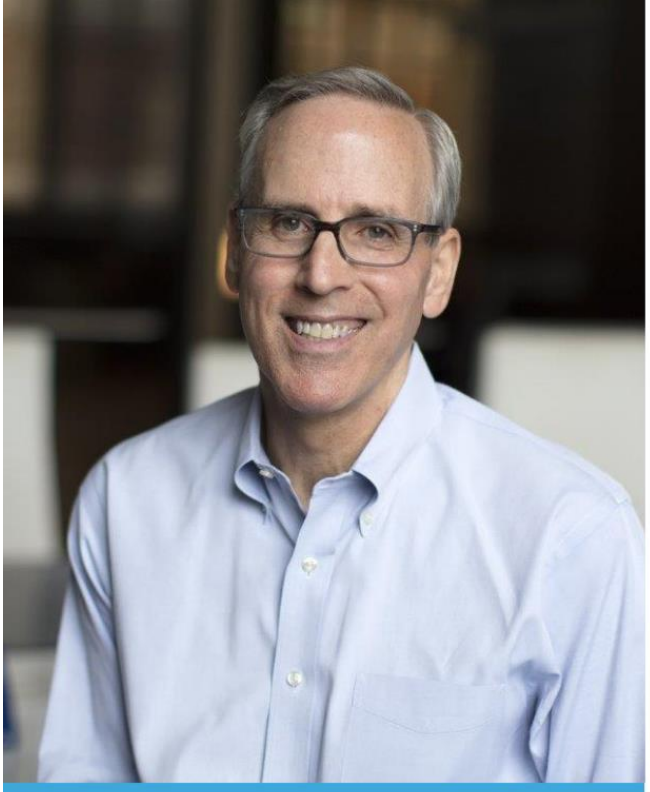

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Jim Routh

ICIT Fellow

The Role of Cybersecurity Leaders as Educators

Unconventional Approaches to Cybersecurity Talent Development and the Scarcity of Skill

AN ICIT FELLOW PERSPECTIVE
MARCH 2022

Introduction

Several decades ago, cybersecurity leaders, then called information security leaders, were accountable for providing a single course on information security for all enterprise employees, encouraging them to act with security awareness. Today, dozens of enterprise stakeholders require unique and specific educational content on cybersecurity practices. Stakeholders include board members, senior executives, IT leaders, DevOps teams, IT auditors, architects, engineers, and analysts, among others. Providing stakeholders with the educational capabilities to learn and practice essential skills is called cyber resilience, and it is a key aspect of cybersecurity. Imagine enterprise cyber resilience as the immune system that relies on behaviors and processes to effectively respond to cyber incidents[5]. This immune system must apply the lessons learned from prior incidents to improve practices and controls, thereby creating a stronger future defense.

Additionally, cybersecurity educational requirements have become increasingly complex since they differ by country. Enterprises within the US must comply with federal, state, and local municipality regulatory requirements. Today's cybersecurity leader must act as an educator who can design and deliver a curriculum that meets the growing complexity of stakeholder and cybersecurity team educational requirements.

According to (ISC)[2], approximately 402,000 cybersecurity jobs in the US go unfilled each year due to the lack of experienced talent[1]. Other sources estimate the range of unfilled cyber jobs to be between 314,000-465,000[2]. The cyber talent shortage in the public sector alone is estimated to be 36,000[3]. Experts predict that the global cyber talent supply must grow by 145% to meet the projected demand from enterprises over the next several years[4]. **Cybersecurity leaders must embrace the responsibility of serving as educators and create and deliver educational curriculums designed to proactively address the talent shortage. Additionally, they must be prepared to meet diverse, and often individually driven, educational requirements for constantly evolving cyber roles.** As a cybersecurity leader, devoting 30% of one's time to talent development is not a widely accepted and established norm today. However, these market conditions mandate the need for a change in focus. A CISO's commitment to talent development actually improves his or her ability to attract talent from outside the organization.

In addition to committing at least 30% of their time to talent development activities for their employees, I believe cybersecurity leaders also need to work closely with HR to apply several **unconventional HR techniques** for talent acquisition and development. I was very fortunate to have the opportunity to work with a few of the most accomplished and innovative HR professionals later in my career[5]. Together, we proved that adopting specific talent management techniques could produce a world-class level of diverse cyber talent. In fact, the vast majority of external candidates who proactively sought roles in these programs did so because of the commitment to talent development by cyber leaders[6].

To start, partner with an HR relationship manager to make the necessary adjustments to both talent acquisition and development practices. Depending on market conditions, these adjustments may be specific to the cyber security team and not the enterprise. For instance, cybersecurity leaders need to hire top talent when they find it, not necessarily when they need it. Cybersecurity talent recruitment must never stop, and hiring freezes due to budget constraints should not be applied to cyber security recruiting activities. Additionally, these recruiting activities should be broad, attracting students in internship programs, undergraduate students, graduate students, early in career professionals, and highly experienced candidates. Most of these activities take years to mature, so stopping and starting

sends the wrong message to the market, eventually impacting the quality and quantity of candidate flow.

Top, diverse talent is challenging for any organization to identify and recruit in the current market conditions. Using continuous, exploratory interviews that are not tied to a specific job posting or job description gives hiring leaders an advantage as these can help leaders understand the ever-shifting nature of potential candidate goals. When a company does need to hire for a specific role, cybersecurity leaders should write job descriptions that sound attractive to candidates without substantial prerequisites, increasing candidate flow and improving the probability of a candidate accepting a role. Job postings should be generic with limited or no pre-requisites or certifications and should not be tied to a specific expiration date. The point is to create a perception in the job market that your company has many potential openings for different skills, and the openings don't disappear. Additionally, roles in your cyber program should be adjusted to allow employees to learn the skills they want. Learning objectives should be defined by the employee, limited to two specific skills, and associated with specific development activities. Having a diverse curriculum that supports this will significantly and positively impact attracting talent to your enterprise. The results from these unconventional techniques include never having to pay recruiting fees, never having a shortage of top, diverse talent, and improving enterprise resilience by consistently developing the next generation of leaders.

As educators, cybersecurity leaders must take advantage of the resources available, both inside and outside their enterprise, to build robust, competent cybersecurity teams and support a data-driven approach addressing the following three levels of management and reporting:

1. **Individual:** Annually, leaders should ask each to identify the two skills they wish to invest in learning and applying. Leaders who understand their employees' desired areas of development, their current competencies, and areas of weakness can provide personalized guidance. By purposefully investing in the development their employees want, employees will be more satisfied with their growth within the organization.
2. **Stakeholder Groups:** This group includes anyone who assesses and mitigates cybersecurity risk within the organization, such as functions, processes, and IT roles. Each has unique educational skill requirements, and it is crucial to understand how people and their associated skills compare to their job functions.
3. **Enterprise in Aggregate:** Enterprise reporting on the transformation of cybersecurity measures over time is valuable for assessing whether your company is moving toward cyber resilience. This larger group of enterprise stakeholders includes the board, senior leaders, investors, auditors, regulators, etc.

How to Effectively Develop Talent as a Cybersecurity Leader

Providing cyber-specific educational content to different internal stakeholders through multiple sources is essential to transforming the behaviors of employees and leaders both inside and outside the cybersecurity program. Over time, effective cybersecurity leaders must influence the behavior of all employees to achieve enterprise cyber resilience.

To attract top, diverse talent in the current market conditions, an organization must invest in a comprehensive curriculum to meet the needs of stakeholders[7]. Cybersecurity leaders need to encourage the cyber program to adjust skills, practices, techniques, and capabilities when cyber threat actors change their tactics. This has implications for your leadership team, cybersecurity employees, employees who report to other leaders but are engaged with cyber program activities, and those accountable for current controls, such as auditors, second-level, operational risk, etc. Establishing a comprehensive and diverse curriculum for multiple stakeholders demonstrates a consistent commitment to providing employees with opportunities to learn new skills, which is essential to attracting candidates at all levels.

Identify and Understand Stakeholders

Developing and maintaining a robust people strategy for your cybersecurity professionals requires understanding the interplay between cybersecurity leadership, HR and learning and development business partners, and third-party vendors and trainers.

Cybersecurity Leaders

It is essential to decouple talent development leadership activities from the conventional performance management model where a leader confirms performance objectives, determines results in a performance appraisal, and provides development feedback. Instead, talent development commitment and activities need to stand apart from performance management. Cybersecurity leaders should spend at least 30% of their time each week on talent development activities distinct from performance and compensation management[7].

Driving transformation must be deliberate. Cybersecurity leaders should identify the appetite of employees to increase their skill levels and then deliver educational resources to meet diverse stakeholder needs, benefiting both the individual employee and the whole enterprise. This process starts with urging employees to identify and document the specific skills they wish to invest their time into learning and mastering.

To support these development objectives, leaders must provide coaching or resources for employees to assess or identify appropriate development activities. Employee ownership of professional development plans is paramount for sustainability and needs to be encouraged by their leader through the organization's commitment to supporting those development activities.

Human Resources and Learning & Development

Larger organizations typically have existing educational resources to help with curriculum design and content delivery, supporting the comprehensive needs of an enterprise cybersecurity training program. Additionally, most cybersecurity leaders use third-party resources that offer unique educational resources so employees can specialize or progress in their roles. Cybersecurity leaders should demonstrate ownership over the content and delivery of educational components from multiple sources to meet the diverse needs of their stakeholders.

Third-Party Vendors and Training Providers

Creating, designing, and implementing a comprehensive curriculum for enterprise stakeholders is a massive undertaking within medium to large enterprises. If cybersecurity leaders lack curriculum

development expertise, they can find those with that expertise to assist them. In particular, leaders should consider the core educational requirements and then add optional content to address diverse learning needs.

Based on my experience, here are some key points to consider when partnering with a third-party vendor:

- Will the training provider work with your organization to understand your key performance indicators (KPIs) and talent development goals for both individuals and teams?
- Does the vendor take a data-driven approach that gives your organization a current snapshot of employees' skills and then allows them to track progress toward their goals?
- Can your training partner support employee career maps and larger workforce development plans that scale with your organizational growth?

The cybersecurity leader, as an educator, must master the design and deployment of many different educational resources that support diverse stakeholder requirements while tracking baseline employee skills to measure progress. The complexity of this across an enterprise is significant. It requires mature tools and partnerships that use a data-driven approach to assess the current state of cybersecurity talent and provide a path to develop skills mapped to personal and organizational goals. At the end of the day, education must demonstrably drive cyber resilience across the enterprise.

To do this, cybersecurity leaders must collaborate with educational experts and HR leaders to consistently enhance educational content for a wide range of cyber skill needs. This will allow companies to effectively compete for talent in the marketplace and internally grow cyber talent[8]. One of the most important KPIs for a cyber program is the percentage of employees who voluntarily left the enterprise and new employees. The ideal range is 2-4% for voluntary departures and 6-12% for new employees. This is a sustainable model for the first few years of a program, with the expectation that the percentage of new employees will taper off as the program matures. It's healthy to have 2-4% voluntary attrition since there are fewer opportunities for specialized and senior talent within a program, and top talent committed to improvement should be encouraged to pursue career growth, even if that leads them outside the company.

Talent Development Practices of the Past and Future

Managers typically identify which employee skills to develop within the performance management process. This choice can be a practical source of information for the employee, but a more effective and unconventional model asks the employee to decide which skills he or she wants to improve. By having employees identify two primary skills they wish to invest in, the professional development dialog is no longer tied to the performance management process. Additionally, the probability of the employee completing these development activities will increase since the employee selected the desired skills.

Cybersecurity leaders should also consider replacing the commonly used term "employee retention" with the term "talent development." **Employees don't have aspirations to be "retained" by the enterprise; they want to develop marketable skills.** Thus, enterprises that demonstrate a commitment to talent development do not need employee retention programs. This new approach ultimately grows talent organically and attracts external talent that wishes to develop marketable skills. The trick is for

enterprises to train cybersecurity leaders to create opportunities for employees to apply learned skills within their roles.

Hiring diverse, top cybersecurity talent in a shrinking labor pool requires another unconventional technique: partnering with HR leaders to specifically hire when talent is available rather than only when the need exists[9]. Rather than posting a single position when needed, recruiting top talent should be a continuous process. Cybersecurity leaders should post generic job descriptions that never expire, encouraging the market to believe that the enterprise is always hiring top talent. This approach may be a source of conflict with HR leadership, but citing the current cybersecurity talent shortage justifies the investment in alternative recruiting strategies.

Making the Business Case for Growing Cybersecurity Talent

There is nothing easy about implementing these unconventional practices. Cybersecurity leaders will encounter resistance at all levels in the organization, even from stakeholders who will benefit shortly. Here are a few points to consider when garnering the support of sponsors and leaders:

- The growth of the cybersecurity talent gap continues to outpace the efforts of university programs, most organizations' current hiring strategies, and external pipeline development programs. This demands that organizations take an unconventional approach to developing talent.
- Continuous recruitment reduces the overall cost of talent acquisition while flexible job roles maximize employee retention. Both practices benefit the individual and the organization.
- When cybersecurity talent is grown organically, organizations benefit from institutional knowledge and relationships developed across other areas of the enterprise.
- Employees value and seek organizations that invest in their development. In turn, employers benefit from hiring candidates who actively seek to work at your organization[10].

Design Principles for the Cybersecurity Leader as an Educator

A cybersecurity leader must demonstrate a commitment to educate diverse stakeholders. This plan must include HR leaders specifically for the unconventional recruiting and development techniques required by the current job market. In two decades of cybersecurity leadership, I never paid a recruiting fee for any external candidate. In fact, when companies only hire from recruiters, this often leads to an insular culture that discourages internal talent from pursuing higher positions at your program. In short, the talent your company acquires will be dependent on your recruiter, and your cybersecurity program should never be dependent on a third party's ability to source talent.

Using my methods, most candidates in a company's pipeline will have approached the company to explore opportunities to expand their skillset. Personally, I used an extensive network of cybersecurity professionals to encourage those wanting to invest in their education to explore the diverse curriculum my company offered to all employees. If that is an attractive outcome for your enterprise, consider these design principles for the cybersecurity team:

1. Hire top talent when found, not just when needed. As such, never stop recruiting activities for any reason. A few "evergreen" job descriptions can continuously attract a broad talent set.

   Rationale: Finding talent in current market conditions must be a continuous process. Stopping and starting recruiting activities yields inconsistent results.

2. Don't seek talent for specific roles. Create or modify roles for candidates and employees based on how they wish to grow their skills and where they can make a significant contribution.
    a. Do an average of five exploratory interviews for internal and external candidates per week.
    b. During interviews, ask candidates what two skills they wish to improve and make a note of the desired skills for each candidate.
    c. Adjust roles to satisfy the learning objectives of employees.

    Rationale: Employees that choose a skill are more likely to learn and apply the skill.
3. Leaders should spend a minimum of 30% of their weekly activities on talent development for cybersecurity professionals and enterprise stakeholders within the organization[11].
    a. Encourage all employees to identify and document the two skills they wish to develop.
    b. Create talent development activities for individual employee development plans.

    Rationale: This is necessary to demonstrate a commitment to talent development for existing and future employees.
4. Develop and maintain a talent pipeline report to identify all internal and external candidates, what they wish to learn, and observations from interviews.

    Rationale: Business conditions and drivers influence resource requirements. A pipeline of interested talent enables an organization to respond quickly to changes in resource requirements.
5. Cyber leaders should create, acquire, and use a broad curriculum designed to meet different stakeholders' diverse learning and delivery requirements in various ways.
    a. Training and education capacity should be governed or enforced by the professional development plan for each employee instead of an amount allocated on a per-person basis.

    Rationale: Individual educational needs for development activities vary greatly and should be driven by individual learning objectives, not by a budget allocation. Additionally, having a diverse curriculum delivery capability, such as gamification, can stimulate employee appetite for learning.
6. Early-career programs designed to funnel students to the enterprise should be developed for a minimum of five years before deciding whether or not to continue the investment. Hackathons are excellent examples of early-career activities that pay long-term dividends.
    a. Increasing diversity and demonstrating inclusive behaviors improves contribution levels and results for the enterprise

    Rationale: Establishing aggressive diversity targets for early-career roles is easier to implement when the enterprise develops and trains employees to have marketable skills.

Conclusion

Cybersecurity leaders need to practice a set of behaviors demonstrating their commitment to talent development principles and practices. They must recognize the requirement to be an educator supporting diverse and multiple stakeholders if they hope to achieve enterprise cyber resilience. It is no longer a "nice-to-have;" it is now an essential skill for cybersecurity leaders to provide education to meet highly diverse requirements for the dozens of key stakeholders in their enterprises. Providing

cybersecurity-specific educational content to multiple internal stakeholders through multiple sources is essential to transforming the behaviors of employees and leaders both inside and outside the enterprise. Internally, it promotes retention, while externally it is a cornerstone for talent acquisition in challenging market conditions. The effectiveness and commitment of leaders as educators has a direct impact on their ability to attract top, diverse talent in the market.

About the Author

Jim Routh is a former CISO/CSO for six industry leading organizations including American Express, DTCC, KPMG, Aetna, CVS and MassMutual. He is the former Board Chair for the Health Information Sharing & Analysis Center (H-ISAC) and the former board member for the Financial Services Information Sharing & Analysis Center (FS-ISAC). He has presented to Boards and Board Committees (Technology & Governance, Audit Committees) for many public and private companies as the CISO or CSO, providing cyber security updates and education designed for board members over the past twenty years. Jim is considered a digital and cyber security industry expert and thought leader. He serves on the boards for Supply Wisdom, GrammaTech, UnBiased Security and the Global Resilience Federation. Jim is currently an advisor for Wiz, Devo, Gurucul, Data Theorem, Cleer Security, Picnic, Badge Security, Saviynt, ThreatDetect and Virsec. He is a faculty member at the NY Tandon School of Engineering where he teaches cybersecurity. He serves in an advisory capacity and investor for four cyber specific venture funds including: SynVentures, CyberStarts, Security Leadership Capital and Rain Capital.

About ICIT

The Institute for Critical Infrastructure Technology (ICIT) is a 501c(3) nonprofit, nonpartisan, and vendor-agnostic cybersecurity Think Tank with a mission to cultivate a cybersecurity renaissance that will improve the resiliency of our Nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders.

Footnotes:

[1] (ISC)[2] 2019 Cybersecurity Workforce Study, https://www.isc2.org/Research/Workforce-Study#
[2] Sources include data collected by the Washington Post under a Commerce Department Grant from August 2, 2021, The Forbes Business Council, October 21, 2021, and Cyber Seek; sponsored by NICE, November 2021
[3] The Washington Post, August 2, 2021
[4] (ISC)[2] 2019 Cybersecurity Workforce Study, https://www.isc2.org/Research/Workforce-Study#
[5] Cyber resilience is a term used to describe the desired state for an enterprise that operates like an immune system for the human body by constantly improving practices, processes, and capabilities to prevent and respond to cybercriminal activity. Improving the behavior of multiple stakeholders with diverse roles is enabled through a commitment to talent development and specifically offering employees opportunities to learn the skills they choose.

[6] When I was the CSO at Aetna, I was fortunate to work with Damien Carter as an HR Relationship Manager. He understood the recruiting challenges for cybersecurity and embraced unconventional practices, such as focusing on talent development, and convinced the HR Leadership Team to make exceptions to established practices.
[7]When I was the CSO at Aetna and CISO at MassMutual, the external candidate flow primarily solicited opportunities to explore opportunities directly with the company instead of being recruited by conventional HR staffing efforts.
[8] xSANS- Build Your Team, https://www.sans.org/build-your-team/
[9] NICE- National Initiative for Cybersecurity Education, https://www.nist.gov/itl/applied-cybersecurity/nice
[10] How to Convince Hiring Managers to work with HR, https://www.shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/how-to-convince-hiring-managers-to-work-with-hr.aspx
[11] The Fifth Discipline: The Art and Practice of the Learning Organization by Peter Senge, 1990 (first edition)
[12] I allocated 30% of my weekly time to talent development activities at three different enterprises over 7.5 years from 2013-2020, and I encouraged direct reports to apply the same allocation (30%) to talent development activities