COSMOS
Navigate the Compliance Universe

CEP Magazine - March 2020
Use the human-centered approach for smarter security and compliance teams

By Steve Durbin

Steve Durbin (steve.durbin@securityforum.org) is Managing Director of the Information Security Forum (ISF), a global nonprofit headquartered in London, UK.

As the cyberthreat landscape becomes more varied and intense in sophistication and strategic intent, demands on information security and compliance teams relentlessly shift and swell. With limited personnel to manage the rising risk, the difficulty attracting, recruiting, and retaining an appropriately skilled workforce has become a risk in and of itself.

Shortages in skills and capabilities are being revealed as major security incidents damage organizational performance and reputation. Building tomorrow's security and compliance workforce is essential to address this challenge and deliver robust and long-term security for organizations in the digital age. Filling the skill shortage will require organizations to change their attitude and approach to hiring, training, and participating in collaborative pipeline development efforts. An overly rigid and traditional approach to identifying candidates, coupled with overstressed and understaffed work environments, is clearly in need of new tactics and fresh ideas.

Organizations that fail to adopt a more creative approach will find themselves dangerously shorthanded in the next few years, as both attacks and defensive measures (e.g., security software platforms, patching and configuration practices, analytics, and machine learning) become more complex.

Today's security and compliance workforce, typically defined as the personnel responsible for an organization's information security and compliance activities, has evolved rapidly since its inception. Over the course of its evolution, the lack of a consensus definition of the information security and compliance functions has allowed numerous, disparate components to form an organization's workforce. For example, employees working within threat intelligence, business continuity, and security operations are all essential information security contributors, yet they rarely convene in one distinct function under a designated leader.

Closing the gap

Closing the gap between supply and demand is imperative for an enterprise to develop an effective security and compliance posture. It is evident that individuals with the required skills, qualifications, and experience are either unavailable or demanding compensation that cannot be met with existing budgets. Because they are in high demand, talented security staff regularly move to new employers as they seek out better salaries and projects at more prestigious companies.

But is this unavoidable? Are hiring managers so inflexible in requiring candidates to have specific skills, qualifications, and years of experience that they end up hindering both their security and compliance teams? Are uninformed and unimaginative recruitment practices contributing substantially to the perceived shortage? As salaries escalate, organizations are urgently seeking a solution to the perceived crisis around hiring information security professionals.

To address the growing demand, organizations should broaden their approach, and work purposefully to recruit security professionals from a diversity of backgrounds, disciplines, and skill sets. Focus on the aptitude and attitude of candidates rather than insisting on a host of specific skills, experience, and qualifications that would eliminate a large portion of current and prospective information security and compliance professionals.

The need for a human-centric approach

As vendors and tools overload the market, potential employees have come to recognize information security and compliance as deeply technical, leaving recruiters struggling to identify and appeal to candidates with a less traditional mix of education and experience. Organizations are swiftly recognizing that bright, diligent, inquisitive individuals are among the most valuable assets an enterprise can leverage. A human-centric approach to information security and compliance will foster a workforce that is capable of meeting the challenges presented by digital risk.

To help achieve a human-centric approach, the information security and compliance functions should collaborate with HR and take advantage of well-established HR practices to build a diverse workforce of capable individuals. A human-centric approach supported by HR provides the structure for a strong workplace culture characterized by proficient and satisfied information security and compliance professionals.

Building a viable workforce

Increasing reliance on digital systems, coupled with a dynamic threat landscape, has made the workforce core to an organization's survival. But for many enterprises, developing a sustainable security and compliance workforce is only an aspiration: attracting and retaining experienced, certified experts is a constant battle.

Organizations need to establish a series of strategic objectives that lay a foundation for a stronger workforce and more robust pipeline. With clear direction and sustained HR efforts, organizations can formalize the structure of the workforce, harness the appropriate talent, and bring security and compliance teams into better alignment with the organization's objectives.

As the security and compliance workforces mature and find innovative ways to embrace the vast resources of untapped talent, the exaggerated myth of a looming crisis in the global workforce will fade. A robust and diverse workforce will empower organizations to face future workforce challenges, such as automation, role and function amalgamation, and increased outsourcing. ISF Members are already demonstrating success at cultivating teams with the necessary skills and expertise in progressive and engaging environments.

A sustainable workforce is essential if the information security and compliance functions are to become partners to the business and effectively manage the increasing cyber risk, security, and compliance burden.

About the author

Steve Durbin's main areas of focus include strategy, information technology, cybersecurity, digitalization, and the emerging security threat landscape across both the corporate and personal environments. Previously, he was senior vice president at Gartner.

Takeaways

- Information security and compliance teams are seeing shortages in skills and capabilities that are being revealed as major security incidents unfold.
- Closing the gap between supply and demand is imperative for an enterprise to develop an effective security

and compliance posture.

- Organizations will need to broaden their approach to attracting talent and work purposefully to recruit security professionals from a range of backgrounds, disciplines, and skills.
- Fostering a workforce that is capable of meeting the challenges presented by digital risk will require a human-centric approach.
- With sustained efforts, organizations can formalize their workforce structure, harness appropriate talent, and bring security and compliance teams into alignment with organizational objectives.