ISACA
1700 E. Golf Road, Suite 400
Schaumburg, Illinois 60173, USA
Telephone: +1.847.253.1545
isaca.org | E-mail: info@isaca.org

The Importance of Certifications in an Evolving Cyber Security Landscape

Addressing the Digital Economic Ecosystem:

Products, Processes, and Professionals

The European Union's 2017 publication of the Cybersecurity Package, including a regulation on European Union Agency for Network and Information Security (ENISA) and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), began an EU-wide discussion on the level of security needed to protect EU businesses and citizens, and to build trust in the Digital Single Market. This has placed cybersecurity at the top of the EU political agenda—a position it should rightfully occupy.

However, the scope of the initial proposal from the European Commission covers ICT products and services; proposed amendments from the European Parliament and the European Council expand the scope of the initial proposal to cover processes. Regrettably, the certification of professionals, currently remains out of the scope of the proposal and its amendments.

ISACA believes that this is a missed opportunity, easily corrected. The strength of the EU's Digital Single Market lies in the hardening of all facets of that digital economic ecosystem—products, processes and, equally importantly, professionals. Additionally, we believe that this is in keeping with the overall commitment the EU and its Member States have demonstrated in their efforts to ensure their respective information and cyber security workforces are filled with well-skilled, high-quality professionals, prepared to tackle the growing challenges of an ever-shifting cyber threat landscape.

Cyber Security Concerns Remain

When ISACA queried Europe's leading cyber and information security professionals for its *2018 Global State of Cybersecurity Research*, it asked respondents if they were experiencing an increase or a decrease in cyber attacks compared to the prior year. Fifty percent of respondents from Europe indicated they were seeing more attacks than the year prior; when queried about how likely it would be that their enterprises would experience a cyber attack in 2018, 80 percent of respondents from Europe believed that the chances of this happening would be either likely (39 percent) or very likely (41 percent).[1] This indicates an environment in which there are concerns about enterprise security. It also indicates that there should be continued emphasis on honing the skills and expertise of the information and cyber security professional community to best address those security concerns.

[1] *ISACA 2018 State of Cybersecurity Survey*

Benefits of Certifications: Employers and Employees

Perhaps the best rationale for the certification of information and cyber security professionals, however, is not about technology, but about the professionals themselves. Affirmation of expertise, skills and abilities by impartial international third parties provides a means of evaluating potential employees, regardless of their location. The mobility of labor, particularly in the EU, is vital to the success of the Union and its Member States, and professional certifications are vitally important in enabling labor mobility while simultaneously ensuring quality.

For professionals, there are multiple benefits. Greater mobility brings with it the ability to expand professional networks and increase knowledge by interacting with peers to exchange knowledge, perspectives, and viewpoints. Similarly, professional certifications serve to improve career prospects and increase earning potential, two assets to any nation or region striving to make its mark in the global knowledge economy.

Employers benefit as well. Professional certifications attest that an employee possesses a certain set of knowledge, abilities, and performance capabilities, all of which are maintained through required training and networking. The class of certifications that include performance-based assessments provide an even greater level of assurance; by requiring the demonstration of skills as part of obtaining a certification, employers also know that a professional can use and apply the lessons they have learned in real-world situations.

Evolving Marketplace, Evolving Role of Certifications

"Certifications," though, deserve an expansive definition. Information and cyber security professionals can already hold various certifications from international organizations such as ISACA. The best of these are vendor-neutral, job-role specific, and globally recognized and accepted. Most importantly, these certifications are aligned to international standards and frameworks, such as those put forth by the International Standards Organization (ISO) or the International Electrotechnical Commission (IEC), and provide an external, impartial confirmation of professional credibility and demonstrated capability.

Recent years, though, have seen a demand for greater variety in the certifications market; now, professionals are able to pursue certificates, digital badges, nano-degrees, and a variety of other credentials. Future discussions of the certification of professionals will need to bear in mind that this space is evolving, but that the foundations of these credentials should remain intact—alignment with ISO or IEC standards and frameworks must remain core elements to ensure adherence to reliable levels of professional excellence and expertise. This has become even more important as millennials increase their presence in the workforce; their prevalence will drive shifts within the certification and credentialing landscape as they explore credentialing options that enable even swifter up-skilling and re-skilling.

Certifications—nearly all credentials, in fact—have a role to play in the educational pipeline as well. A recent article in the MIT Technology Review[2] focused on Germany's *Ausbildung*, and how vocational training in Germany is beginning to shift. As advancing technologies spur faster changes within the digital economy, workers trained to solve problems—rather than those just focused on one or several discrete tasks—likely will be those who fare best. Germany's *Ausbildung* has taken note of this and taken steps to create alternative educational pathways that marry the best of vocational training with the best of traditional university educations. It is not difficult to imagine the role certifications and other credentials could play in this and similar constructs, with certifications, certificates, badges, and the full gamut of micro-credentials serving as educational milestones along the educational journey.

[2] MIT Technology Review June/July 2018 Issue; Rebuilding Germany's centuries-old vocational program; R. Juskalian

Along the entirety of the professional's journey—from early career interest at the pre-university and university levels, through continuing professional education—certifications and all credentials have a role to play in ensuring that knowledge, expertise, skills and abilities are measured in an open, transparent and standard manner. As the workplace continues its evolution within the global digital economy, the need for maintaining relevance and competency will become even more critical; credentials can, will, and should be a foundational component of efforts to meet that need.

We can no longer think in terms of only people, or processes, or products; we must think in terms of how all three of those elements come together and interact as interdependent parts of an ecosystem. Within such an environment, certifications and credentialing play a critical role, augmenting strong processes, and making exceptional products even better.

Conclusion

It is paramount that, going forward, discussions regarding the Cybersecurity Package also contain consideration of the certification of professionals. As the EU seeks to strengthen its Digital Single Market and the entire region's digital economic ecosystem, well-trained professionals in information and cyber security will be increasingly important to support those efforts.

As the marketplace evolves, so do its needs; some elements, however, are foundational. There will always be a need for employers to know they are employing highly-skilled, top-quality professionals. Similarly, there will always be a need for employees to retain and grow their relevance in their chosen fields of interest. Certifications and credentialing are a single solution that addresses both needs.

ISACA believes that a wide-ranging public policy discussion of certifications and their role in both the workforce and the educational pipeline would be of immense benefit to the EU and the future of the Digital Single Market, and our organization stands ready to participate in such discussions. It would be worthwhile for the EU to explore the possibilities of cybersecurity as a vocation, with certifications and credentialing serving as critical components in these learning pathways. It is ISACA's strong belief that a constantly changing landscape of ever-evolving technologies and threats makes certifications, credentialing, and continued professional education more important than ever.

About ISACA

ISACA helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association representing approximately 160,000 information and cybersecurity professionals in nearly 190 countries. As part of ISACA's efforts to support the global IT professional community, ISACA offers COBIT®, a business framework to govern enterprise technology, and the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource to assist organizations in developing skilled cyber workforces and enabling individuals to grow and advance their cyber careers.