CISO Strategy

Should Cybersecurity Leadership Finally be Professionalized?

The majority opinion is that a cybersecurity professional body is long overdue and would benefit cybersecurity and cybersecurity practitioners.

By

Kevin Townsend

April 29, 2024

Professionalization could be a solution to the increased cybersecurity risk for corporate and national security; and the mental health and even physical liberty of CISOs. But it's not easy.

Professionalization for cybersecurity leadership has long been mooted but never actioned. Times are changing. The CISO role has expanded and become critical for both individual companies and national security. Threats to personal mental well-being have escalated, and CISOs can be held criminally liable for corporate security failures.

In 2013, the National Research Council (NRC) published *Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decision-Making*. The NRC's conclusions were negative: cybersecurity is too dynamic to establish a baseline of requirements; the knowledge and competencies required are too extensive to allow professionalization; and in an age of cybersecurity skills shortage, professionalization could provide additional barriers for entry.


Martin Zinaich, CISO for the City of Tampa.

Within two years, Martin Zinaich (CISO at the City of Tampa) advocated for professionalization in a separate paper titled *What does Information Security have in common with Eastern Air Lines Flight 401*?': "The largest benefit [of professionalization]" he wrote, "comes from elevating the field into the business arena, where businesses are aware of, better understand the role of, and are able to fit Information Security into the proper level of business process… When the current ad-hoc approach is exchanged with a holistic approach, it benefits the business, the industry, the consumer, and the nation."

Zinaich's views are as relevant and accurate today as they were a decade ago – but the NRC's view has prevailed. It is time to revisit these arguments in detail.

Reasons to now professionalize

Counterintuitively, one of the main arguments in favor of a professional body is the rapidly increasing complexity of cybersecurity (the same complexity that has been used to avoid professionalization in the past), and the exposed and vulnerable position of its leaders. The applications CISOs use and protect are more complex and contain more bugs. Adversaries are more sophisticated and more aggressive in exploiting these bugs. Criminal gangs are better organized while elite nation state hackers seek to steal intellectual property and national security information, sow discord among populations, and disrupt critical industries.

While cybersecurity leaders must defend against these external adversarial threats, they are also effectively attacked from within. They are insufficiently resourced, must rely on security tools that are often inadequate and bring new vulnerabilities into the mix, have responsibility often without adequate authority, are forced to commit sparse resources on complying with complex

national and international regulations that do little or nothing to increase security, and are easily scapegoated if things go wrong. And now, with the new and confusing SEC disclosure rules, face criminal liability and even jail time if they make a mistake.

“CISOs are in the unique position of facing potential legal repercussions, including civil or criminal liability,” comments Darren Guccione, CEO and co-founder at Keeper Security.

A cybersecurity professional body could serve three fundamental purposes. Firstly, through lobbying (vendors for better tools, and governments for more realistic and achievable regulations). Secondly, by supporting members (for more corporate authority, and resources), and defending members faced by company scapegoating or federal charges for nothing more than a mistake. And thirdly, in improving the general level of cybersecurity by raising standards and practices.

Amanda Finch, CEO of the Chartered Institute of Information Security (CIISec).

“A rising tide lifts all boats, and increased professionalism in the cybersecurity industry can only be a good thing,” suggests Amanda Finch, CEO of the Chartered Institute of Information Security (CIISec) in the UK. (We’ll have more to say on the CIISec in the section on potential professionalization models.)

“Major industries such as healthcare, accounting, law, banking and many more have standards bodies in place,” she continues. “These have really transformed those sectors, enabling them to self-govern with an agreed standard of service. This has helped to protect customers and has given structure to the workforce. Cybersecurity must follow suit in the US.”

Malcolm Harkins, chief security & trust officer at HiddenLayer, agrees. “And it should have occurred long ago,” he adds. He believes that professionalization is necessary not merely to improve the quality of security practitioners, but to protect the integrity of professionals. He notes that in the last few years, business responsibility and regulatory requirements have increased while budgets have flatlined or reduced.

“Many CISOs I know understand their ‘duty of care responsibilities’ and act that way – sometimes, unfortunately, at the risk of losing their job for not ‘going along’ with a management approach that adds risk rather than appropriately managing it… We cannot kick the can down the road anymore. It’s time to act by creating more accountability, and it’s time to lead and codify the CISO role to manage the risks that need to be managed.”

Wish list for a professional body

There are many natural outcomes from professionalizing cybersecurity (such as improving standards, simplifying recruitment, and formalizing a career path for future leaders). However, a professional body could achieve far more: advocating for better regulations and improved products, and providing a safety net for exposed members.

Regulations pressure group

Most CISOs accept the need for regulations but suffer from their strictures. Governments are slow in developing rules. Regulations are often a compromise between satisfying political opponents, not upsetting big business, and national security lobbying – and they are usually a reaction to history rather than a commitment to the future (consider how the arrival of AI has triggered a sudden rush for new regulations on a new technology that nobody really understands).

The SEC disclosure rules are a good example of a bad regulation. The purpose is clear and largely acceptable, but the wording and potential sanctions are worrying. What does a ‘material cybersecurity incident’ mean; and is jail time a reasonable punishment for a genuine mistake?

“Should CISOs have the concept of a Safe Harbor?” asks Sasa Zdjelar, chief trust officer at ReversingLabs. The medical profession has this concept. “If a doctor does everything right, he can still lose a patient – but will have some protection from the medical profession.” There are similar protections in the legal profession.

A safe harbor would be more likely with the support of a cyber security professional body, operating in the same way as the medical and legal professions. A professional body could help governments frame better regulations, and defend CISOs from bad regulations.

Liability insurance

Associated with (but not limited to) bad regulations could be the practical support to individuals offered by a professional body. This could take numerous forms – but examples could be negotiating and even funding personal liability insurance for members. In the event of criminal charges, such support could include legal support.

What, for example, could be the effect of an amicus brief from a pool of potentially tens of thousands of the country’s most qualified cybersecurity professionals?

Such an amicus brief, suggests Zdjelar, could say, “This CISO did nothing wrong. He or she acted with best practices and in good faith. He or she acted transparently, and this prosecution is unfair and unjust. And because of this, the Cybersecurity Professional Board will bring its $*nn* million liability umbrella policy to bear on a legal defense.”

Product pressure group

“A professional body could set minimum product requirements,” suggests Zinaich. “It could lobby or develop a Cyber Underwriters Laboratory (which actually exists, but no one knows about it) and tag products and services with such validations.”

An independent product evaluation laboratory would highlight security product weaknesses and failings. Vendors would be forced to improve their products or face a mass snub from the professional body’s members.

Reasons not to professionalize

Despite all the advantages and discussions, we are no closer to professionalizing cybersecurity in the US than we were 15 years ago. It is important to understand the reasons.

Complexity

Narayana Pappu, CEO at Zendata, believes that the NRC arguments from 2013 still hold true today. “While there is an opportunity for standardization of the CISO role with better cross functional education (a CISO can’t be just a technologist anymore) he/she needs to understand the business as well as understand functions and operations of CIO and CDO roles,” he says.

“The creation of a professional body is not a way to solve the problem. Such bodies usually have a high barrier to entry and don’t account for places with substantial risk but no resources (mid-market and small businesses). Finally, they are slow to adapt, which is just the nature of having a process/committee.”

His preference would be, “cross collaboration with existing CISO bodies, with online certification that is in reach for SMBs, and collaboration with entities representing CIOs and CDOs.”

Inertia

It is 17 years since the founding of the UK’s Institute of Information Security, and ten years since Zinaich called for US professionalization. There is continuous discussion and support for the idea of a cybersecurity professional body – but no visible progress in the US. It may partly be caused by the complexity and ever-changing role of the CISO, including the multiplicity of jurisdictions within which international corporations must operate. It may partly be due to the large number of small companies with CISOs who feel they have little influence either inside or

outside of their companies. It may be because of a multitude of influencing factors. But they all accumulate into one overriding physical law: inertia.

Overcoming inertia may be the biggest obstacle to the professionalization of the cybersecurity workforce. Outside of government – and, frankly, government should remain outside of this process – there is no existing body with sufficient intent and strength to overcome this inertia and get the ball rolling.

Potential professional models

Professional Engineering Model

Omri Weinberg, co-founder and CRO at DoControl, suggests looking at the Professional Engineering license model as the basis for a cybersecurity profession. “In most US states, as well as in other parts of the world, a PE license or equivalent is required for certain areas of higher responsibility, like approving plans for structures of buildings or bridges, overseeing environmental impact studies and reports, or even teaching engineering at the collegiate level.”

He believes the model has characteristics comparable to the needs of the cybersecurity profession. “[The PE model] has both broad, multidisciplinary components as well as specific areas of focus for its certification process. PEs must demonstrate foundational knowledge across multiple disciplines in engineering as well as expert level understanding of their particular focus areas.”

Omri Weinberg, co-founder and CRO at DoControl.

Further, the requirements for gaining the license could easily translate to cybersecurity: a relevant formal education, passing a general examination, four years of mentorship from a licensed person, a focused exam after the mentorship, and “specific training on the ethical and societal ramifications and responsibilities that license holders have.”

To further the argument, he adds, “Engineering is already adjacent to Computer Science/Information Systems in most universities; so, extending the engineering licensing model to cybersecurity makes sense, where a model like for medical or law practitioners might fit less well, especially in the early stages and for beginners in the field.”

Medical/Legal Professions

Zinaich proposed using the medical profession as a blueprint for professionalization a decade ago. He didn’t accept the ‘too complex’ argument. At the time he noted a paper published by the Pell Center (*Professionalizing Cybersecurity: A path to universal standards and status*) that said the American Board of Medical Specialties has 24 general certificates and 125 subspecialty certificates. “In terms of depth and breadth, Information Security does not appear to be any more complex than other professionalized occupations,” comments Zinaich.

Harkins also recommends the medical (and legal) professions as a starting point. “At the end of the day, I have always believed CISOs have a ‘duty of care’ to their shareholders, their customers, and to society, depending on who is impacted by a cyber risk. In healthcare, ‘duty of care’ refers to the responsibility of healthcare providers to ensure that they act in the best interests of the individuals that they care for, perform their work competently and not do anything that could result in harm to others. In the legal context, if you also don’t act in the interests of your clients and within the law, you can be disbarred and removed from being a practicing attorney.”

Malcolm Harkins, chief security & trust officer at HiddenLayer.

Apart from maintaining and promoting professional standards, there are further advantages to these models. Firstly, they are operated by experts in the field rather than government or government agencies. Secondly, they are not proscriptive. Customers are not required to employ a qualified member of the professional body: patients could choose to use a nutritionist, herbalist, acupuncturist, or homeopath rather than a medical doctor; plaintiffs and defendants could represent themselves or be represented by an unqualified friend.

Companies, then, could choose to employ a CISO based solely on knowledge of the applicant or strength of a CV rather than accredited membership of a formalized body.

Zdjelar looks to the legal profession as a source for inspiration. “Every state has its own Bar Association,” he comments. “That’s a private organization, not a government organization, that polices itself. Qualified members of that society of attorneys decide who can be newly qualified attorneys. And if existing members act in a way that’s not consistent with best practices or disrespects the profession, they will disbar them or remove their ability to practice law in that given state.”

Key comparable elements here are, firstly, the professional bodies are non-governmental – it is professionals setting the standards for professionals. Secondly, each state has its own Bar Association, making the body jurisdictional. This is important since each state has its own laws, and is comparable to cybersecurity where different jurisdictions, both state and international, have different security regulations.

There remain problems that make a direct correlation with either the legal or medical professions impossible. Cybersecurity is dynamic and changes rapidly. Law changes far more slowly.

In the medical profession, you could say there are two elements: the human body and medicines. The first changes very little: evolution is a slow process. Medicines change more rapidly with the release of every new drug. This model is similar to cybersecurity, where human anatomy would relate to IT infrastructures and medicines would relate to both cyberattacks and cyber defenses.

The rapid technology changes reduce the value of academic qualifications. For example, the rapid emergence of cloud technology caused a scramble for cloud-qualified engineers – and there weren’t any because all formal training predated the cloud concept. The same is likely to happen – or is already happening – with AI. There will always be advances in technology, and formal academic training will struggle to keep pace.

“To me,” says Zdjelar, “professionalization doesn’t equate to a university degree or to some sort of formal education. But I think it should demonstrate knowledge. It’s a body that says, ‘You need to demonstrate proficient knowledge in these domains. And have someone who is an active practitioner with the same sort of knowledge confirm you were observed practically applying these skills for, say, *x* period of time.’ Entry into the professional body would be via a champion or endorser. I see a cybersecurity professional body as something more akin to that than a professionalization that comes with the formality of university degrees.”


Sasa Zdjelar, chief trust officer at ReversingLabs.

Chartered Institute of Information Security (UK)

Steve Benton, VP of threat research at Anomali, is a Fellow at the UK's Chartered Institute of Information Security (CIISec). The institute was founded in 2006 "to address the problem of how to recognize a competent information security practitioner." It was granted a Royal Charter of Incorporation in December 2018 by Queen Elizabeth II.

"This body has been formed to sustain a holistic approach for the professional development of all layers and levels from analysts up to CISO," says Benton. "As a Fellow, I can attest to the drive and impact of the Institute (some 35,000 members). It is doing just the right things across the holistic approach, and I would offer this as a model for the US with CISO professional development at the top."

Finch adds, "We've seen the success of standards bodies in the UK's cybersecurity industry. It's given the security industry a voice, as well as a community of other like-minded professionals to network with. We've also worked with our members to create key initiatives, such as chartering and a skills framework, which are setting benchmarks for the industry and improving processes and practices across the board."

Gareth Lindahl-Wise – London, UK-based CISO of California-headquartered Ontinue – also advocates for a CIISec type model. "If I as an individual or institutional recruiter will favor, or demand, membership of such a body as a selection criterion, then a critical mass will develop in a much shorter time. The benefit to the recruiter is obvious, access to a pool of trusted and assured talent wider than my own network."

Membership of that professional body includes peer review. "I am firmly in favor of an organization which maintains its integrity through genuine peer review of applicants and has a focus on senior security leader challenges," he adds.

Creeping professionalization imposed by expanding government regulations

Our final option for professionalization is to do nothing and allow current processes to continue. This is the haphazard government-led imposition of professional standards through the legal exclusion of what government considers to be bad behavior rather than the encouragement of good behavior as understood by practitioners.

Governments are slow. They have their own priorities (economy and national security, both of which can lead to apparent contradictions in the application of rules). They have a better understanding of threats than of the practical problems companies have in implementing mitigations to those threats.

Government regulations often cause confusion and difficulty. The SEC disclosure rules (admittedly only applying to public companies) are an example. Disclosure is required; but what, when and why isn't adequately defined or explained. And if a CISO's good faith understanding of the requirement doesn't align with the inadequately undefined opinion of the SEC, it could lead to criminal liability. (See the *CISOs, SEC, and the liability curveball* section of *Cyber Insights 2024: A Dire Year for CISOs?* for a discussion on the potential effects.)

The possibility of government-instigated professionalization would be detrimental to the cybersecurity profession. Indeed, this possibility is really another argument in favor of a practitioner-led professional body – it could help government bodies better understand the operational complexities of cybersecurity and lead to better regulations if and where they are needed.

Summary

The majority (not exclusive) opinion is that a cybersecurity professional body is long overdue and would benefit cybersecurity and cybersecurity practitioners. The success of the UK's CIISec demonstrates that it can be done. But the problems remain – not the least being who would define the 'good practice' that would be supported by the profession?

The complexities highlighted more than a decade ago by the NRC are increasing. But so is the need. The role and responsibilities of the CISO are expanding. The pressure to do more with less resources while navigating the often contradictory demands of sustaining business profitability without becoming liable for regulatory failures is increasing. The role of the CISO needs support while the liability of the CISO needs defense. These would be best delivered by a non-governmental independent professional body.

There is a potential route that can be traced through our discussions: an organization largely modeled on the US medical and legal professions, but with entry based more on peer review and demonstrable current expertise than on a formal education. This resonates with the overall existing cybersecurity culture.

Nevertheless, the biggest obstacle remains: an inertia that gets more intractable with each passing year. It is difficult to imagine any single source of energy, outside of government, with enough power to overcome this inertia. “Professionalization could help clarify the roles, responsibilities and expected competencies of cybersecurity professionals, thereby reducing ambiguity and potential liability,” says Guccione. “However, the mammoth task of imposing such requirements may be impractical for an industry already navigating a dynamic threat environment.”

Written By Kevin Townsend

Kevin Townsend is a Senior Contributor at SecurityWeek. He has been writing about high tech issues since before the birth of Microsoft. For the last 15 years he has specialized in information security; and has had many thousands of articles published in dozens of different magazines – from The Times and the Financial Times to current and long-gone computer magazines.