Reconsider the Australian Government's grant for professionalising the cybersecurity industry

Author: Benjamin Mosse

Date: 27/01/2025

Acknowledgements:
I wish to sincerely thank Andrew Horton, Beverley Roche, Christopher Flynn, Corch, Christian Heinrich, Daniel Grzelak, Dan Maslin, Dave Worthington, David Cheal, Edward Farrell, Elliot Seeto, Duncan Hart, Elliot Dellys, Eric Eekhof, Eric Pinkerton, Georgina Crundell, Grae Meyer-Gleaves, James Taylor, James Davis, Jamieson O'Reilly, Jarrod Loidl, John Ellis, Kiranraj Govindaraj, Mel Kendell, Michael Collins, Michael Glowacki, Mike Loss, Mike Trovato, Neil Curtis, Nick Ellsmore, Nigel Phair, Paul Watters, Filip Palian, Rob Parker, Shane Moffitt, Simon Willgoss, Theo Nassiokas, Wayne Tufek and all the other members of our community that shared their points of view.

CONTENTS

EXECUTIVE SUMMARY

Minister Anthony Burke, Lieutenant General Michelle McGuinness,

The purpose of this paper is to share a synthesis of 40 perspectives from senior Australian cybersecurity leaders about the proposed professionalization of our field. While many of these viewpoints express varying levels of concern about the scheme, this paper is not an attack on the grant or the scheme. Instead, it is an earnest attempt to provide thoughtful and constructive insights that you can use to help ensure the success of this important project.

I understand that the 2023-2030 Australian Cyber Security Strategy includes a recommendation to professionalize the industry, with an active $1.9M grant to design, test, and promote a national, self-sustaining cybersecurity professionalization scheme.

In response to this grant, Mr. Tony Vizza and Mrs. Jill Slay published an open-source proposal aimed at offering "evidence-based, expert guidance to the Australian governments, industry and academia stakeholders in relation to establishing a professional accreditation scheme for the Australian cyber security workforce."

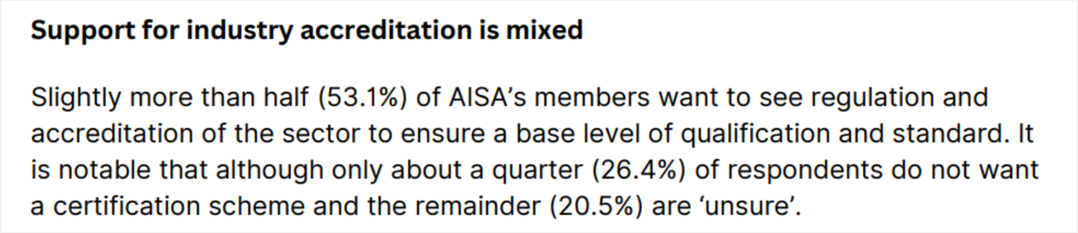
Following the publication of this proposal, 40 senior cybersecurity leaders shared their points of view on LinkedIn. I used that data to perform a sentiment analysis which revealed that 7.5% of them are firmly in favour of the scheme, 2.5% mostly in favour, 15% are 'in the middle', 50% mostly against and 25% firmly against.

The key themes identified from their perspectives are as follows:

Theme #1: There is mixed support for a professionalization scheme

In addition to the Sentiment Analysis in this paper, a 2022 AISA survey found that 53.1% of members supported regulation and accreditation, 26.4% opposed it, and 20.5% were unsure, indicating divided opinions within the industry.

This means that the scheme is at risk of not being adopted by at least 1 in 2 cybersecurity professionals – possibly more than that.



Support for industry accreditation is mixed

Slightly more than half (53.1%) of AISA's members want to see regulation and accreditation of the sector to ensure a base level of qualification and standard. It is notable that although only about a quarter (26.4%) of respondents do not want a certification scheme and the remainder (20.5%) are 'unsure'.

Source: Research into Cyber Security Accreditation, AISA, September 2022, page 6

Theme #2: Many are concerned that vested interests will hijack the scheme

There seems to be no consensus on the best entity to implement the scheme – ideas include non-profits, government agencies, or quangos. Leaders also raised ongoing concerns about risks of vested interests. This suggests that senior leaders view the risk of the scheme being hijacked by vendors or unscrupulous parties as very high, which could pose a significant threat to the entire industry and the success of this project.

> *"Mandating an Australian cybersecurity certification will create a supply line for a demanded product, being the Australian cybersecurity certification. It will also create significant demand if this certification is mandated as a condition of being able to perform specific cybersecurity roles. The immediate conclusion is that while I can't say if certificate holders or the cyber industry will benefit from this scheme, the certain beneficiaries will be the businesses and organisations that successfully integrate themselves into the Australian cybersecurity certification supply line, as they will benefit financially."*
> *Theo Nassiokas, Founder of Cyber8Lab, ex APAC CISO at Berclays*

> *"I would say that some people who are pushing a specific single scheme also hold executive or governance roles where there's a clear conflict of interest that is not typically disclosed"*
> *Honorary Professor Dr. Paul Watters and vCISO*

Theme #3: The scheme oversimplifies a deeply complex profession

Cybersecurity is an exceptionally complex and dynamic field, with frameworks like NIST NICE identifying over 50 work roles and DoD Directive 8140 listing more than 70—and these numbers continue to grow. The field encompasses numerous distinct domains of expertise, and it is uncommon for individuals to master even a few, let alone all, of these areas, particularly given the rapid pace of change.

Simplifying job credentials into broad categories such as "associate," "principal," and "chartered," tied to pre-selected certifications, degrees, and years of experience, oversimplifies this complexity. Such an approach fails to capture the diverse roles, specialized domains, and competencies required of cybersecurity professionals.

If the goal of the professionalization scheme is to clarify individual competencies, this kind of oversimplification may have the opposite effect: create more confusion and undermine its intended purpose of providing clarity.

> *"Having been responsible for looking at large-scale cyber workforces, including Whole of the Victorian Government with 350,000+ total staff [...]. I am firmly of the opinion that there are many different skillsets that consist of being a Cyber Professional."*
> *Shane Moffitt, ex CISO of the Victorian Government*

Theme #4: There's a misalignment between the scheme's goals and proposed solutions

Expectations for the scheme are widely varied, ranging from:

a) improving classroom education
b) increasing the availability and quality of teachers
c) increasing gender diversity
d) establishing ethical standards
e) removing underperforming or delinquent actors from the marketplace
f) either creating or eliminating barriers to entry (depending on whom you ask)
g) and many other claims

These diverse objectives make the scheme's goals overly ambitious.

This lack of clarity suggests that, for many, the scope of the professionalization scheme is uncertain, making its value equally unclear. A poorly defined scope risks either failing to achieve its goals or focusing on the wrong objectives, ultimately preventing the intended value from being realized.

> *"As a proponent for professionalization for my entire 45 year career - for professional services firms - I have supported industry and professional associations globally, the qualifying and certification/credentialing of my team and clients. But is this something we need for the everyone? Just professional services? Again, what problem are we solving?"*
> *Mike Trovato, Managing Partner at Cyber Risks Advisors, ex EY and KPMG Partner*

> *"Sounds like there's a big disconnect between the goals and the path to reach them. There's a lot of this in our industry. We do things that feel like they should work and make us feel like we are doing something but in practice don't achieve their outcomes"*
> *Daniel Grzelak, Chief Innovation Officer at Plerion, ex CISO of Atlassian*

Theme #5: The scheme's return-on-investment (ROI) lacks evidence

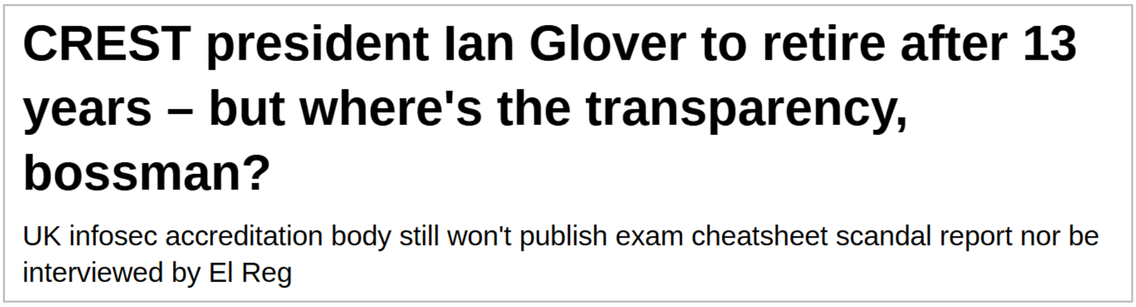
There is no clear, first-hand evidence to show that a professionalization scheme for the cybersecurity sector can effectively address or alleviate the root causes of the problems it seeks to solve. This means the scheme might be set up to fail from day one.

> *"How does a professionalisation scheme solve the real challenge of making Australian businesses more secure?"*
> *John Ellis, Global Head of Security at QBE, ex CISO at Bupa*

> *"While attempts to uplift the profession are always welcome, they should be guided by clear evidence in terms of both efficacy, priority with a clear and achievable mandate."*
> *Jarrod Loidl, Director at Deloitte*

Theme #6: Malicious actors will game the system without mastering the skills

Past cheating scandals, such as the CREST UK cheating incident, highlight risks of the malicious actors finding loopholes in the system to gain a marketplace advantage:



CREST president Ian Glover to retire after 13 years – but where's the transparency, bossman?

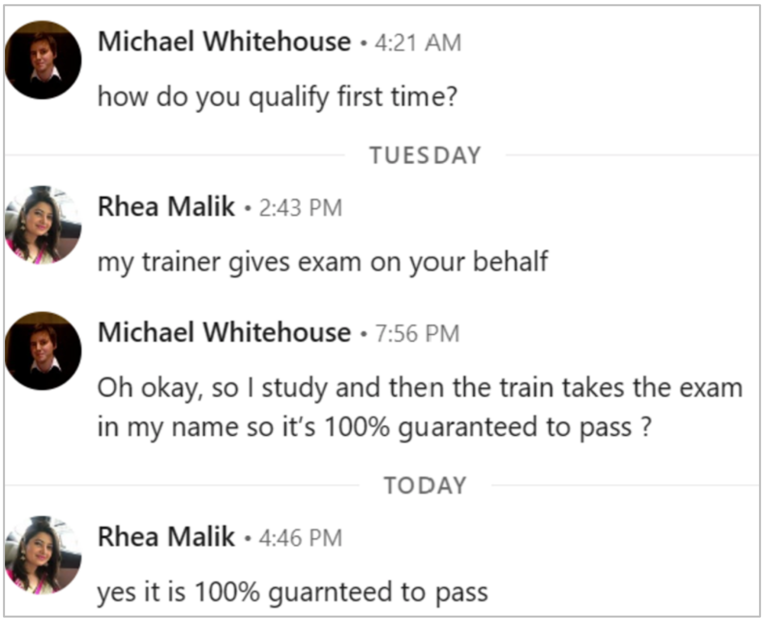
UK infosec accreditation body still won't publish exam cheatsheet scandal report nor be interviewed by El Reg

Source: Gareth Corfield, The Register, Fri 18 Jun 2021

> *"People who worked hard to pass their CREST exams expressed disgust to El Reg that a significant backer of the industry body appeared to be spoon-feeding its staff the answers, raising questions about the exams' integrity and the competence of people who ultimately sign off clients' crown jewels as secure. Those clients include the British government and critical national infrastructure operators."*
> *Gareth Corfield, The Register*

If the goal is to ensure that individuals accredited under the scheme are truly competent, but the scheme is easy to cheat, then it has fundamentally failed. Even worse, a cheating scandal could tarnish the reputation of the entire cybersecurity profession and undermine decades of effort spent building credibility across business, government and society.

Here's a screenshot from LinkedIn of a bad actor taking industry tests for a fee:



Michael Whitehouse • 4:21 AM
how do you qualify first time?

TUESDAY

Rhea Malik • 2:43 PM
my trainer gives exam on your behalf

Michael Whitehouse • 7:56 PM
Oh okay, so I study and then the train takes the exam in my name so it's 100% guaranteed to pass ?

TODAY

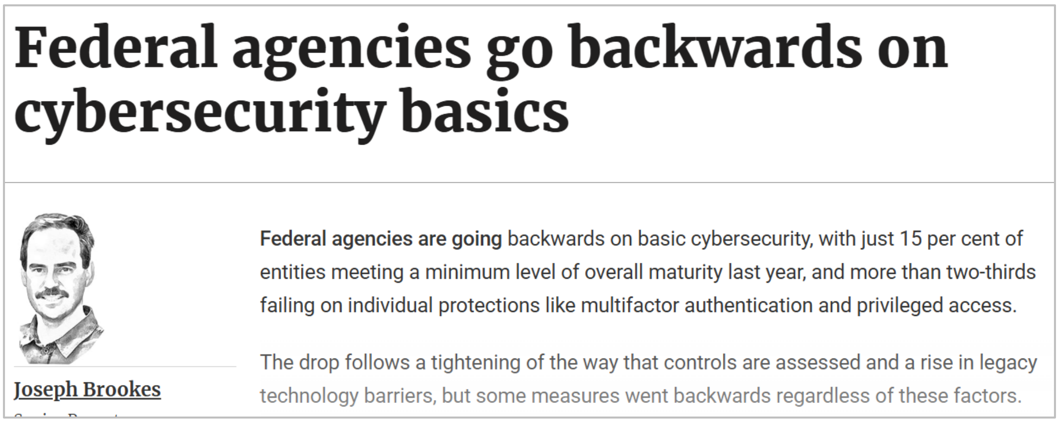
Rhea Malik • 4:46 PM
yes it is 100% guarnteed to pass

Theme #7: The scheme ignores the broader context within which professionals operate

Cybersecurity professionals lack not only the legal backing but also the enforcement mechanisms at all levels to ensure secure practices are upheld.

Voluntary frameworks such as those proposed by associations (e.g., the ACS) rely on employer goodwill and carry no penalties for noncompliance. Consequently, organizations often ignore basic security measures – like enforcing multi-factor authentication – because it's cheaper or more convenient, leaving ethical practitioners helpless or risking their careers by "blowing the whistle."

Moreover, current legislation is rarely enforced, enabling companies to treat breaches as tolerable risks rather than obligations. Even the Australian government resists adopting its own cybersecurity standards.



Federal agencies go backwards on cybersecurity basics

Joseph Brookes

Federal agencies are going backwards on basic cybersecurity, with just 15 per cent of entities meeting a minimum level of overall maturity last year, and more than two-thirds failing on individual protections like multifactor authentication and privileged access.

The drop follows a tightening of the way that controls are assessed and a rise in legacy technology barriers, but some measures went backwards regardless of these factors.

Source: Joseph Brookes writing for InnovationAus on the 7th of January 2025

In the absence of robust legislative enforcement and binding industry standards, efforts to 'professionalize' cybersecurity might not achieve its goal of improving the protection of both ethical practitioners and the public.

> *"Cyber security won't be a certifiable profession before we are charging $600 per hour, held personally liable for poor advice, hold professional indemnity insurance at a cost exceeding $20,000 per annum and CISOs/board members are held criminally liable for reckless and negligent security decisions."*
> *Dale J., Consultant and ex Chief Security Architect for the ATO*

Conclusion

While this executive summary highlights what I believe to be the top 7 concerns raised by senior leaders, I have collected a total of 28 unique criticisms (see Appendix B). This suggests to me that more consultation is needed. I encourage you to conduct further research, gather more insights, and, given the divisive nature of this issue, take steps to deepen everyone's understanding of both the benefits and how the risks will be addressed. I believe it would be wise to resolve these uncertainties before awarding the grant.

DETAILED RECOMMENDATIONS

If, after reviewing this document, you agree that support for the professionalization scheme is mixed and at least some of concerns raised by the senior leaders are valid, then I encourage you to conduct further research, seek additional consultation, gather more feedback, and deepen everyone's understanding before proceeding with the grant.

Step 1: Do more search and learn more

1.1. Collect insights from 300 senior leaders to formally capture all the pros and cons of a professionalization scheme

1.2. Publish a whitepaper summarizing the key viewpoints to educate the community

1.3. Clearly define the scope of what Australia's professionalization scheme might be, and provide first-hand evidence that it can achieve its intended goals

1.4. Determine how the professionalization scheme will address each problem within the selected scope, supported by evidence

1.5. Analyse evidence from seven (7) other professions where similar schemes have succeeded or failed, and extract key lessons learned

1.6. Resolve implementation challenges and ensure the scheme is safeguarded from vested interests

1.7. Identify additional investments required to effectively resolve the stated problems

Step 2: Write a compelling business case

Develop a compelling business case that adheres to best practices, with a well-defined scope, evidence-based solutions, thorough risk assessments, realistic benefits, and alignment with stakeholder needs.

- Is the scope properly defined—broad enough for ROI, yet narrow enough to ensure success?
- Does the business case address the root causes of the identified issues?
- Are the benefits realistically presented, or have they been overstated?
- Has a thorough risk assessment been conducted, and have key risks been mitigated? Are risks transparently addressed, or have they been downplayed?
- Are assumptions and limitations clearly outlined?
- Have all key stakeholders been consulted and are they aligned?
- Is the business case both feasible and viable?

Step 3: Convince the Australian cybersecurity community with evidence and goodwill

3.1. Publish the business case, gather feedback, and remain open to iteration until all major criticisms are addressed

3.2. Organize nationwide presentations at conferences and panel discussions, allowing your team to engage face-to-face with the community and build support for the new version of the scheme

3.3. Conduct a survey via AISA, demonstrating that at least 80% of the community supports the scheme after being fully informed

Step 4: Reopen the grant application and evaluate applications

4.1. Reopen the grant application process to allow all interested parties to submit or refine their proposals

4.2. Evaluate each application thoroughly, focusing on feasibility, evidence-based solutions, and alignment with industry needs

4.3. Scrutinize proposals rigorously to ensure they can realistically achieve the intended goals

4.4. Avoid selecting an applicant simply for the sake of progress; ensure the proposal is well-founded and viable

4.5. If no proposal is ready for effective execution, delay the decision, refine the approach, and wait for the right conditions to move forward

4.6. If you select a proposal, then release it for public review and commentary

APPENDIX A — COMMUNITY RECOMMENDATIONS

Below are ideas from the senior leaders that may help refine and improve the concept of a professionalization scheme. I've always found the community to be incredibly helpful and motivated to solve problems. Even those who seem to oppose progress provide counterpoints that deserve thoughtful consideration.

Author	Point of View
Beverley Roche	"we need an independent agency to govern not and industry association"
Christopher Flynn	"before we attempt to make Cyber Security a profession, we need to pursue Duty of Care and fix the dangerous End User License Agreement first"
Edward Farrell	"I'd deduct an apprentice - journeyman - master model which I've advocated might be suitable" "as a practitioner, I want to be onboard. I also want domains that do not require technical rigour to be apart of such as scheme as their actions also have an impact and require some form of conduct." "multiple associations and industry bodies have a say in this scheme and have already done most of the work." "Building on what's already been done."
Eric Pinkerton	"To do it properly we will need to establish a Quango to provide the oversight"
Filip Palian	"Why the entire industry though? Start with the government itself and GRC and see how it works out for you."
Hardik Cholera	"In my opinion government representative like ASD can chair the discussions with public/private partnership with global forums across the world. AISA certainly can be the face of Australian Information Security Council with other such Not for profit bodies from around the world as main participants. The benefit of this would be same global language rather than we always referred to as 'this is how they (we) do things down under'"
John Ellis	"The heart of cyber security lies in people: their curiosity, adaptability, and commitment to learning. Using myself as an example, as I progressed into senior roles, broadening my skills through AICD and board service helped me align with understanding my stakeholder and their needs. Any professionalisation scheme must follow this principle — serving both the profession and those who rely on us."
Grae Meyer-Gleaves	"Consultation would need to be 360 and include boards, regulators, shareholders, customers and many other stakeholders. […] Needs to be all in and collaborative, balanced and fair. But it needs to also have a clear objective/purpose and reason."

Author	Point of View
Michael Glowacki	"Education, self learning and on the job experience is already in place. Its about working together and upskilling that is the piece missing from certifications. Cyber is an ever changing environment, with new techniques and new threat vectors, this requires hands on, real time experience. We as an industry cannot wait a year or longer for people to certify or re-certify as we need get on the ground now." "I agree that a council is needed, both from a governance perspective, but also as a centralised place of learning and sharing of knowledge."
Michél Nguyễn	"we need also need a speaking organ like a council for security guys/ladys. Overall unity is required and forum to discuss and create global guideline(s)."
Mike Trovato	"As a proponent for professionalization for my entire 45 year career - for professional services firms" (Mike says he thinks the scope should be professional services)
Nick Ellsmore	"there are 3 different things that a "professionalisation" scheme is generally trying to "validate" about a person, of differing levels of importance/value to different participants in the process: 1. Knowledge - do you know a certain baseline of stuff 2. Practical Expertise - can you apply that knowledge 3. Integrity - can we trust you with significant access"
Rob Parker	"there needs to be a sustained long term investment to actually make a difference."
Theo Nassiokas	"If it could be designed to: (a) keep quality of cyber professionals high without impeding supply of what is already a chronic industry shortage of cyber security professionals; and (b) designed in a way that it benefits the certification holder more than the businesses that issue the certification, then that's great!"
Wayne Tufek	"We already have elements of a professional scheme such as exisiting certifications (notably ISACA ones!) I think any money is better spent educating the market in what to look for and the questions to ask and aimed specifically at those that do not know how to spot a reputable supplier."

APPENDIX B — RESEARCH METHODOLOGY

Sentiment Analysis Overview

Between Monday, January 20, and Saturday, January 25, 2025, 40 senior leaders shared their perspectives on the proposed professionalization scheme for Australia's cybersecurity sector. I reviewed and categorized their views into four groups:

1. **Firmly in Favor**: Leaders who explicitly support the scheme with no criticisms.
2. **Mostly in Favor**: Leaders who expressed more support than opposition, liking the idea overall but raising one or several notable concerns.
3. **In the Middle**: Leaders who provided a balanced perspective, weighing both the pros and cons more or less equally.
4. **Mostly Against**: Leaders who strongly opposed the scheme by raising concerns and criticisms without explicitly rejecting it outright.
5. **Firmly Against**: Leaders who explicitly opposed the professionalization scheme.

Sentiment Analysis Results

Firmly in Favour	Mostly in Favour	In the Middle	Mostly Against	Firmly Against
Elliot Seeto	Elliot Dellys	Beverley Roche	Christopher Flynn	Andrew Horton
James Davis		Edward Farrell	Christian Heinrich	Benjamin Mosse
Nigel Phair		Eric Pinkerton	Daniel Grzelak	Corch
		Grae Meyer-Gleaves	Dan Maslin	Dave Worthington
		Mike Trovato	Duncan Hart	David Cheal
		Nick Ellsmore	Eric Eekhof	Dale J
			James Taylor	Georgina Crundell
			Jamieson O'Reilly	Jarrod Loidl
			John Ellis	Shane Moffitt
			Kiranraj Govindaraj	Wayne Tufek
			Mel Kendell	
			Michael Collins	
			Michael Glowacki	
			Michael Loss	
			Neil Curtis	

Firmly in Favour	Mostly in Favour	In the Middle	Mostly Against	Firmly Against
			Paul Watters	
			Filip Palian	
			Rob Parker	
			Simon Willgoss	
			Theo Nassiokas	
3	**1**	**6**	**20**	**10**
7.5%	**2.5%**	**15%**	**50%**	**25%**

Limitations of the Sentiment Analysis

I acknowledge all the limitations of this sentiment analysis. First, it is based on my interpretation of publicly posted points of view, which is inevitably influenced by my own biases. Furthermore, none of these leaders were interviewed in depth, so I cannot claim to fully understand their true perspectives. In some cases, some leaders just expressed a strong support and agreement for someone else's point of view. Second, the sample size is limited to just 40 individuals. Therefore, the only firm conclusion I can draw from this sentiment analysis is that support for the professionalization scheme is mixed, and further research and consultation is necessary.

Extracting the Criticisms, Rebuttals and Possible Refutations

The true value of this work lies in distilling the criticisms and rebuttals of senior leaders who have earnestly articulated their reasons for opposing, in part or in full, the professionalization scheme. Those firmly or mostly in favour of the scheme would do well to fully engage with these critiques to refine and improve their concept.

Ultimately, if the criticisms contain a single refutation which decisively demonstrates that a professionalization scheme cannot work in cybersecurity, then the opinions, numbers, or evidence on either side become irrelevant. Therefore, the most important question is whether the scheme can withstand rigorous critical scrutiny?

1. Top Themes:

Below are the top 7 themes that I have identified and documented in the Executive Summary and will only highlight in this section:

1.1. There is mixed support for a professionalization scheme

1.2. Many are concerned that vested interests will hijack the scheme

1.3. The scheme is oversimplifying a deeply complex profession
1.4. There's a misalignment between the scheme's goals and proposed solutions
1.5. The scheme's return-on-investment (ROI) lacks evidence
1.6. Malicious actors will game the system without mastering the skills
1.7. The scheme ignores the broader context within which professionals operate

2. Other Criticisms:

The following other criticisms were raised:

#	Critique	Proof / Evidence
2.1	Proposals for the professional schemes tend to overstate the benefits and downplay the risks. They also do not list their assumptions and limitations.	Tony Vizza and Jill Slay's proposal
2.2	Professionalization schemes justify in part their existence by citing poor cybersecurity degrees and certifications as a problem, yet they include these same credentials as part of the solution. How can the problem also be the solution? If the goal is to improve cyber education, then this seems like a devastating internal contradiction.	Tony Vizza and Jill Slay's proposal
2.3	It seems that human performance follows a Power Law. For example, 1000 individuals can get accredited on an ethical hacking certification but only 5-15% can truly hack real-world software. Therefore, if the goal is to measure, manage and predict human performance, then titles, credentials and years of experience are poor indicators.	This research paper among many others that can be provided
2.4	If the goal of a professionalization scheme is to prevent delinquent actors from participating in the cybersecurity marketplace, then, by definition, the scheme is a new barrier to entry – contradicting the claim that the scheme will remove barriers to entry.	Pure logic
2.5	The professionalization scheme is far from a national priority.	
2.6	Egos and fractured opinions within the industry are major obstacles to adopting a professionalization scheme.	This document AISA's 2022 survey
2.7	$1.9M is barely enough to get started, let alone guarantee a success long-term execution.	
2.9	Most cybersecurity incidents are caused by non-cyber professionals mismanaging technology through poor risk management, misconfigurations, or insufficient budgets.	Postmortem analysis of major cyber incidents
2.10	In a rapidly evolving field, it's nearly impossible to define a consistent body of knowledge to certify against.	Never ending stream of emerging technologies, techniques, tactics and tools
2.11	It seems the professionalization scheme lacked thorough consultation, with boards, regulators, shareholders, customers, and other key stakeholders left out of the process.	Absence of evidence that thorough consultation occurred

3. Rebuttals

I have also collected rebuttals to arguments in favour of the professionalization scheme:

#	Argument in favour of the scheme	Rebuttal
3.1	Many industries, like medicine and law, have professionalization standards—so why shouldn't cybersecurity follow suit?	Many sectors thrive without professionalization. For example: data science, system administration, software development, marketing, and sales – amongst hundreds of other examples.
3.2	The cybersecurity industry, like the medical profession, plays a critical role in safeguarding lives and systems, which is why it requires a professionalization scheme.	It's been pointed out that this argument might be a false equivalency. Unlike medicine, which requires years of structured study and cannot be self-taught, cybersecurity often thrives on self-taught talent. Junior professionals are frequently more up to date on the latest tools and techniques than their senior counterparts. Furthermore, the adversaries who successfully bypass our security operate without professionalization standards, proving that competence in this field is driven by adaptability, ingenuity, critical thinking, continuous learning, and grit—not by checklists or rigid frameworks.
3.3	Something is better than nothing. We need to start somewhere.	It's been pointed out that this argument might fall into the trap of the politician's fallacy: assuming that creating new processes and paperwork automatically signifies progress. This overlooks the risks, assumptions, criticisms, and refutations that must be addressed for genuine improvement.
3.4	If I was trying to procure services in this space as a small company, I'd have no idea who to trust – that's why we need a professionalization scheme.	There is no first-hand evidence a professionalization scheme reliably signals true competence, capability, or ethics — it merely identifies who can pass a checklist.
3.5	If a professionalization scheme is managed by a non-profit, it reduces the risk of exploitative fees and monopolization in the free market.	It's been pointed out that vendors and large players can easily dominate non-profit boards, using their influence to serve their own interests. Some say this happened to AISA a few years ago.

4. Ad Hominem Arguments

Ad hominem arguments, when used thoughtfully, can provide valuable insights into the motivations and biases of individuals advocating for a particular idea. Understanding *who* is making an argument and *why* they may hold their position can help uncover potential conflicts of interest, hidden agendas, or inconsistencies that might otherwise go unnoticed. While they should not replace substantive critiques, ad hominem arguments can complement logical analysis by providing context that deepens our understanding of the debate.

Here are some of the ad hominem arguments that I have collected as part of this review:

4.1. It seems that those who advocate most fervently for a professionalization scheme are often the ones with the least hands-on experience and proven competencies in the field.

4.2. "Monkey see, monkey do" is no justification for disrupting an entire sector without proving ROI or addressing valid criticisms.

4.3. It seems that some advocates for professionalization schemes are succumbing to the politician's fallacy: "Something must be done; this is something; therefore, it must be done."

4.4. It seems that advocates of professional schemes cannot even meet basic industry standards to secure their own websites, raising the question: should they themselves be granted titles and credentials that claim competence?

4.5. It seems that some of the strongest advocates for the professionalization scheme refuse to lead or take responsibility for its execution, shielding themselves from the risks they impose on others—a telling sign that these schemes are fraught with risks, downsides, and a high likelihood of failure.

Performing Your Own Analysis

In Appendix D, I have included most of the data I used for this review. To fully understand the context, I encourage you to follow the links, read the complete threads and even contact the senior leaders yourself to clarify any misunderstandings.

I want to sincerely apologize for any errors I may have made. Despite my best efforts and due diligence, I know I am not immune to mistakes. I welcome and encourage anyone who wishes to cross-evaluate my analysis to do so. Any errors on my part were made in good faith, with the best of intentions, and I deeply appreciate your understanding and constructive feedback.

APPENDIX C — MY THOUGHT PROCESS, MOTIVATIONS AND OPINIONS (SHOULD YOU CARE)

I oppose the professionalization scheme, but perhaps not for the reason you might expect. Over the past three days, I've discussed the scheme extensively with peers, and one thing stands out: many evaluate the scheme by weighing its pros and cons. Their method consists of some sort of mental and emotional calculation which weighs the goodness of the idea and their degree of belief towards the arguments for and against.

As a result, some end up on positions such as "this might be better than nothing," "at least we're doing something," "perfection is the enemy of good," or "if the rewards outweigh the risks, it might be worth doing."

The challenge is that evaluating the professionalization scheme based on how good it seems to one person versus another prevents us from correcting errors and therefore hinders the evolutionary process that the idea must go through for true progress to occur.

I therefore reject this method entirely—not to dismiss their perspectives, but because I believe it uses the wrong criteria (epistemology). Instead, I follow a "Yes or No Philosophy," where I evaluate ideas based on whether they withstand decisive criticism.

If an idea cannot achieve its stated goal within a given context, it is refuted, and we should never act on refuted ideas, no matter how promising they may seem.

This might sound radical, but as highly influential philosopher Sir. Karl Popper and acclaimed physicist David Deutsch teach: all knowledge is conjectural. The best ideas are those that work at solving a problem and for which no refutations are known.

This philosophy forces me to think critically and try falsifying ideas rigorously. Only when I find no critical faults, after thorough research and reflection, do I fully endorse an idea. I also embrace the view that decisiveness through a clear "yes or no" and holding a firm, well-researched opinion are virtues in life. I have little respect for tentativeness, playing it safe, attempting to please all sides, or worse, pleasing authority figures. I take ideas very seriously and go "ALL IN" on the very best ones.

In the case of the professionalization scheme, I believe that the current version of the idea has been decisively refuted. It cannot reliably determine whether someone is competent in cybersecurity if that's the goal. For example, if 1,000 people earn an ethical hacking certification, only a small fraction—perhaps 5% to 15%—are truly capable at such craft in the real-world. Therefore titles, credentials, and years of experience are unreliable indicators of competence because the distribution of human competency is uneven – it in fact follows a Paretian Distribution.

Another refutation that I believe undermines the entire project is this: proposals identify inadequate degrees and certifications as part of the problem. Yet, these same credentials are, a few pages later, included in the scheme's framework as part of the solution. But how can a part of the problem also be a part of the solution? This internal contradiction reveals that these schemes fail to hold themselves accountable to their own analyses, claims and goals.

Much like Friedrich Nietzsche, I also have a taste for good ad hominem arguments (because human psychology matters) and find it telling that the scheme's proponents avoid addressing the criticisms and rebuttals of 37 senior leaders head-on, either with evidence or pure logic.

In direct opposition to their behaviour, let me address the primary criticism of me made by my detractors—that I have a vested financial interest in opposing the scheme. They're right about the financial interest, but not as they imagine. My cybersecurity institute stands firmly against legacy and mostly theoretical, degrees, certifications and courses that are part of the problem and endorsed by their frameworks.

Ironically, their insistence that some certifications are of higher quality because they are certified ISO/IEC 17024 only validates my stance and improves my credibility. This naturally drives interest and revenue to my real-world method, as professionals eventually recognize that real-world problem-solving and critical thinking are essential for career success.

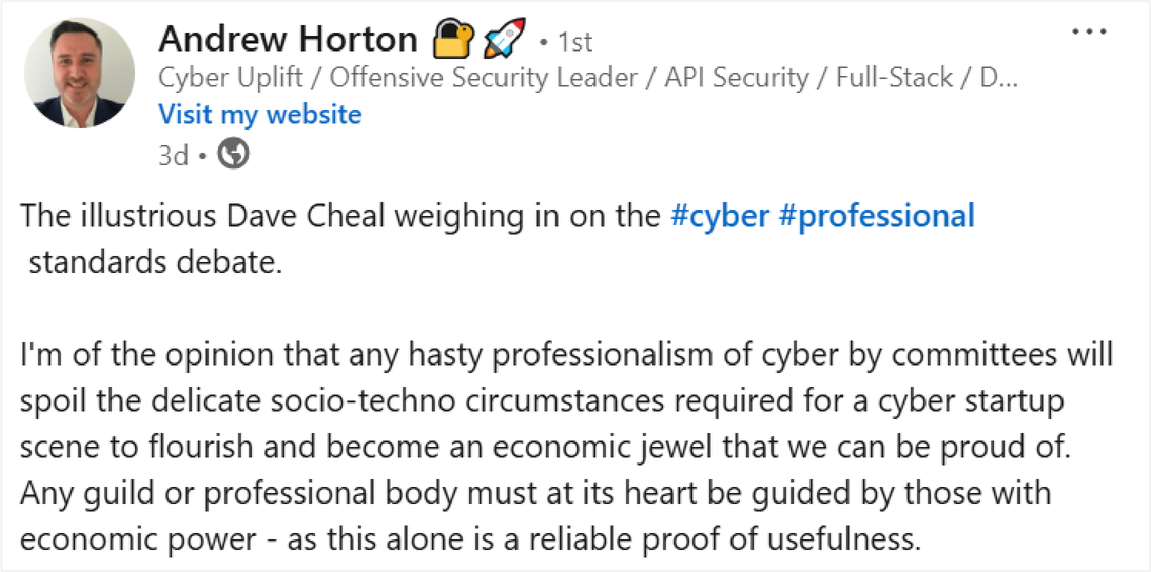
Furthermore, the idea that ISO/IEC compliance is a signal of course quality is laughable and those who make such claims are embarrassing themselves. To me, it shows that my fiercest opponents are utterly detached from the needs and realities of most cybersecurity leaders.

As a closing statement, I oppose this scheme not out of cynicism but because I believe we must act only on ideas that solve big problems, are feasible, viable and unrefuted. Anything less is a disservice to the progress we all seek. I remain open to the possibility that the idea for a professionalization scheme could evolve into something I might endorse in the future—provided that all major criticisms are decisively addressed and resolved.

APPENDIX D — PUBLIC RECORDS

Andrew Horton, Co-Founder at ThreatCanary (15 years of experience)

On the 20th of January 2025, Andrew published this:



Andrew Horton 🔐🚀 • 1st

Cyber Uplift / Offensive Security Leader / API Security / Full-Stack / D...

Visit my website

3d • 🌐

The illustrious Dave Cheal weighing in on the #cyber #professional standards debate.

I'm of the opinion that any hasty professionalism of cyber by committees will spoil the delicate socio-techno circumstances required for a cyber startup scene to flourish and become an economic jewel that we can be proud of. Any guild or professional body must at its heart be guided by those with economic power - as this alone is a reliable proof of usefulness.

Source

Benjamin Mossé, CEO of Mossé Security and MCSI (20 years of experience)

On Monday the 20th of January 2025, Benjamin Mossé published this:

I debated Tony Vizza on his proposed scheme for Australia's cybersecurity sector. I presented 3 rebuttals and faced ad hominem responses. Ultimately, Tony deleted our conversation to hide the refutations from the public.

It's crucial for all Australian cyber professionals to read my arguments, as the scheme would impact everyone. Please share this post with your peers.

My first two criticisms target the proposal. If you accept even one, then you should reject the proposal:

1) It lacks references to case studies, research, or metrics that prove a professionalization scheme can lessen the issues listed on pages 4–6. Despite many sectors having such schemes, Tony and Jill found no first-hand evidence that it would improve education quality, increase gender diversity, or produce better teachers, among other claims.
2) The proposal fails to discuss its assumptions, risks, and limitations. It overstates benefits, downplays risks, and cherry-picks information to suit its goals. Known risks about stifling innovation, creating barriers, and incentivizing wrong behaviours are not discussed.

My 3rd criticism challenges the idea of a scheme outright. Accepting this argument implies we should abandon the project:

a) Human performance follows a Power Law rather than a normal distribution. A small number of people produce most of the innovation and results ("80/20")
b) If the goal is to measure and predict performance, then titles, credentials, and years of experience are poor signals
c) Thus, the scheme cannot achieve its goal
d) It will tell us who "passed the checklist," not who is truly competent

Ref: https://lnkd.in/gm9r4ekc

I quote the abstract:

"We conducted 5 studies involving 198 samples including 633,263 researchers, entertainers, politicians, and amateur and professional athletes. Results are remarkably consistent across industries, types of jobs, types of performance measures, and time frames and indicate that individual performance is not normally distributed—instead, it follows a Paretian (power law) distribution"

"Assuming normality of individual performance can lead to misspecified theories and misleading practices"

"our results have implications for all theories and applications that directly or indirectly address the performance of individual workers including performance measurement and management, [...] and the prediction of performance"

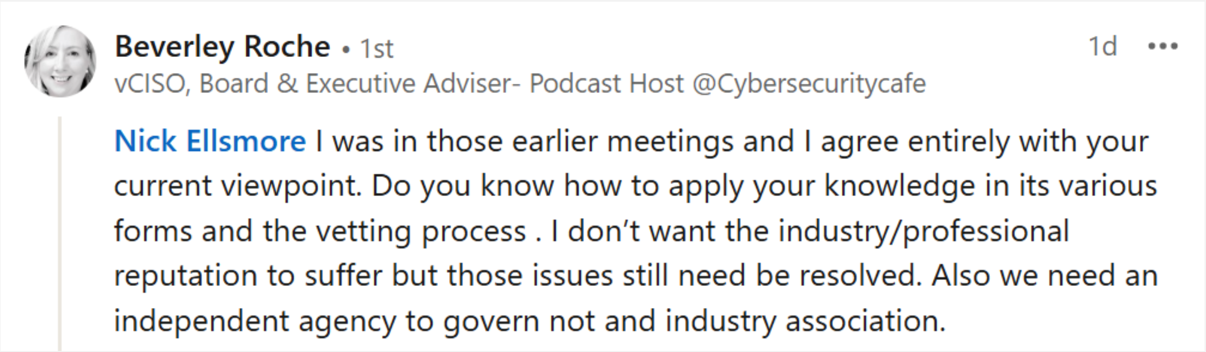
I now offer a new, immanent critique that reveals a decisive internal contradiction:

a) The scheme aims to unify multiple elements under a single framework (diagram on page 10)
b) However, the problems identified in the analysis coexist with these elements
c) Some elements even contribute to the problems. For example, degrees that poorly prepare students for employers are included
d) Therefore, the scheme fails to address the root causes and doesn't hold itself accountable to its own claims

Source: https://www.linkedin.com/feed/update/urn:li:ugcPost:7286830209801035777/

Beverley Roche, Cyber Executive at CyberRisk (20 years of experience)

On the 21st of January 2025, Beverley published this:



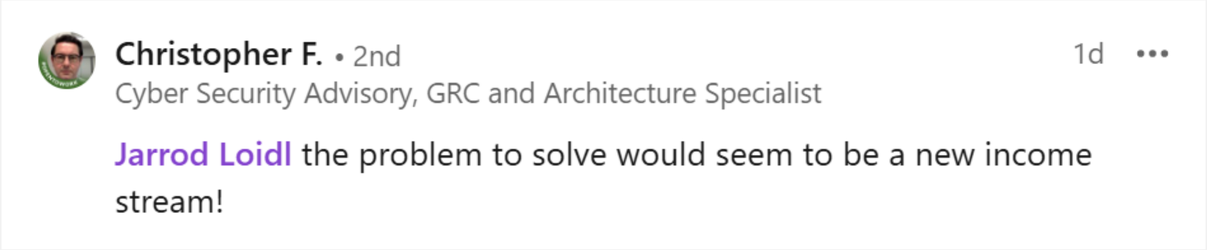
Beverley Roche • 1st
1d •••
vCISO, Board & Executive Adviser- Podcast Host @Cybersecuritycafe

Nick Ellsmore I was in those earlier meetings and I agree entirely with your current viewpoint. Do you know how to apply your knowledge in its various forms and the vetting process . I don't want the industry/professional reputation to suffer but those issues still need be resolved. Also we need an independent agency to govern not and industry association.

Source

Christopher Flynn, Cyber Security Realist at Sphaera (40 years of experience)

On the 21st of January 2025, this is what Christopher published:



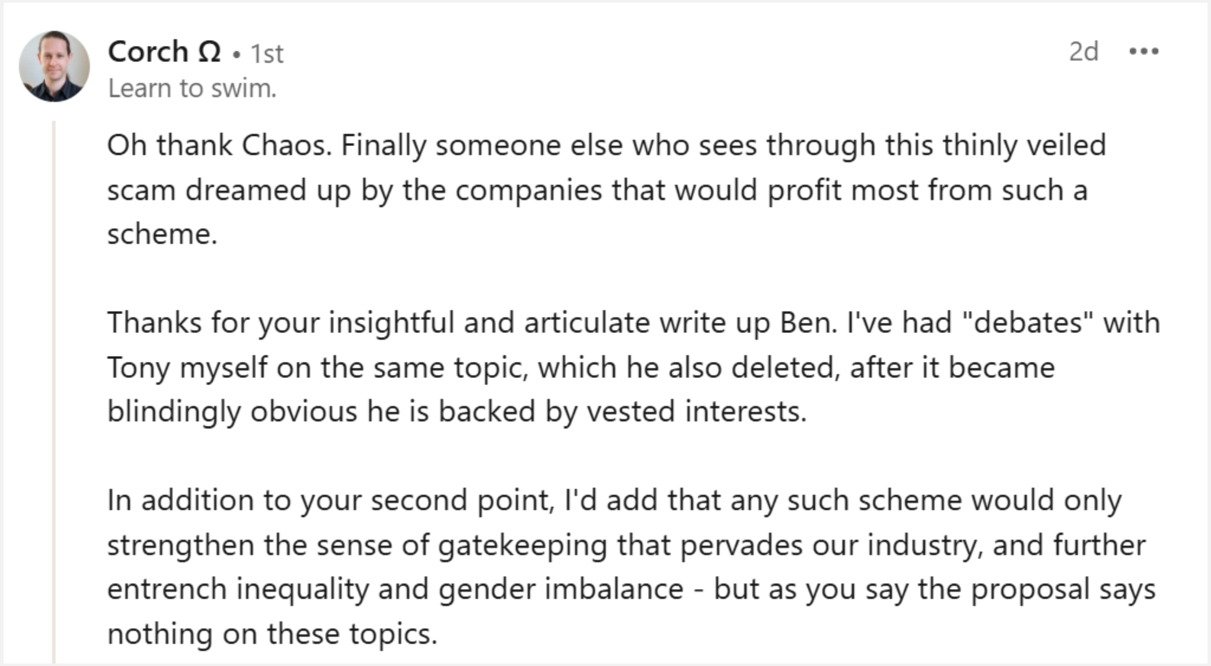
Christopher F. • 2nd
Cyber Security Advisory, GRC and Architecture Specialist

1d •••

Jarrod Loidl the problem to solve would seem to be a new income stream!

Corch, Chief Trouble Shooter at Shogun Cybersecurity (20 years of experience)

On the 20th of January 2025, this is what Corch published:



Corch Ω • 1st
Learn to swim.

2d •••

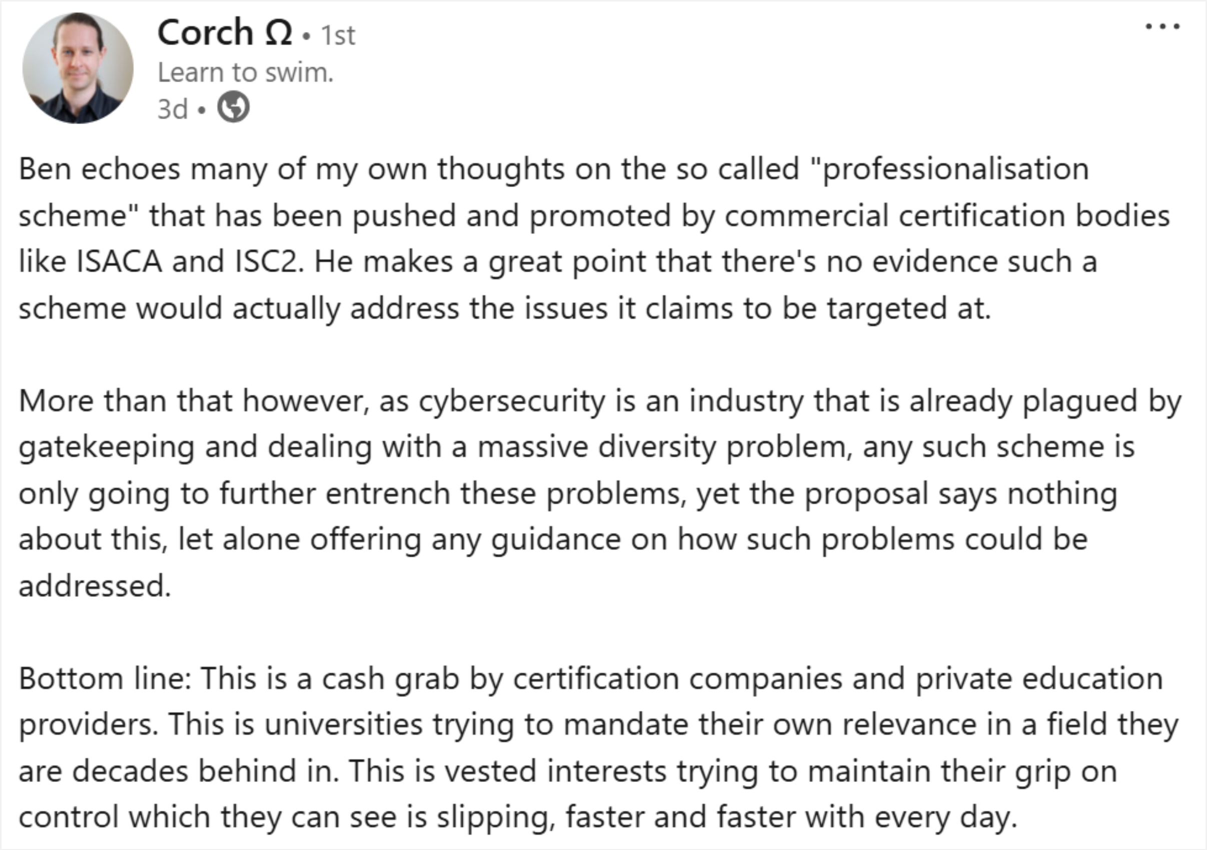
Oh thank Chaos. Finally someone else who sees through this thinly veiled scam dreamed up by the companies that would profit most from such a scheme.

Thanks for your insightful and articulate write up Ben. I've had "debates" with Tony myself on the same topic, which he also deleted, after it became blindingly obvious he is backed by vested interests.

In addition to your second point, I'd add that any such scheme would only strengthen the sense of gatekeeping that pervades our industry, and further entrench inequality and gender imbalance - but as you say the proposal says nothing on these topics.

Source

He also wrote this:



Corch Ω • 1st
Learn to swim.
3d •

Ben echoes many of my own thoughts on the so called "professionalisation scheme" that has been pushed and promoted by commercial certification bodies like ISACA and ISC2. He makes a great point that there's no evidence such a scheme would actually address the issues it claims to be targeted at.

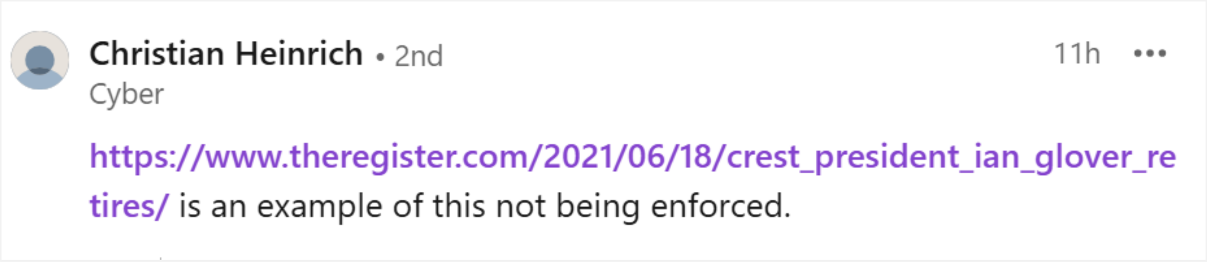
More than that however, as cybersecurity is an industry that is already plagued by gatekeeping and dealing with a massive diversity problem, any such scheme is only going to further entrench these problems, yet the proposal says nothing about this, let alone offering any guidance on how such problems could be addressed.

Bottom line: This is a cash grab by certification companies and private education providers. This is universities trying to mandate their own relevance in a field they are decades behind in. This is vested interests trying to maintain their grip on control which they can see is slipping, faster and faster with every day.

Source

Christian Heinrich, Cyber at CONFIDENTIAL (26 years of experience)

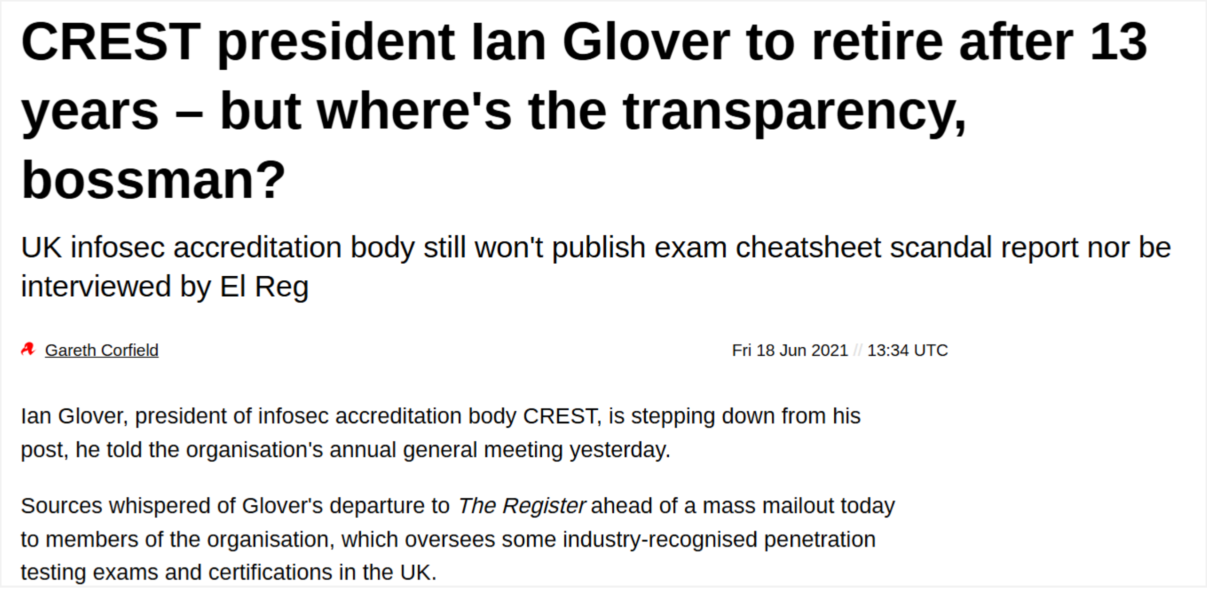
On the 22nd of January 2025, Christian published this:



Christian Heinrich • 2nd 11h
Cyber

https://www.theregister.com/2021/06/18/crest_president_ian_glover_retires/ is an example of this not being enforced.

Christian reported that in 2021, the UK information security accreditation body, CREST had faced a cheating scandal:



CREST president Ian Glover to retire after 13 years – but where's the transparency, bossman?

UK infosec accreditation body still won't publish exam cheatsheet scandal report nor be interviewed by El Reg

Gareth Corfield Fri 18 Jun 2021 // 13:34 UTC

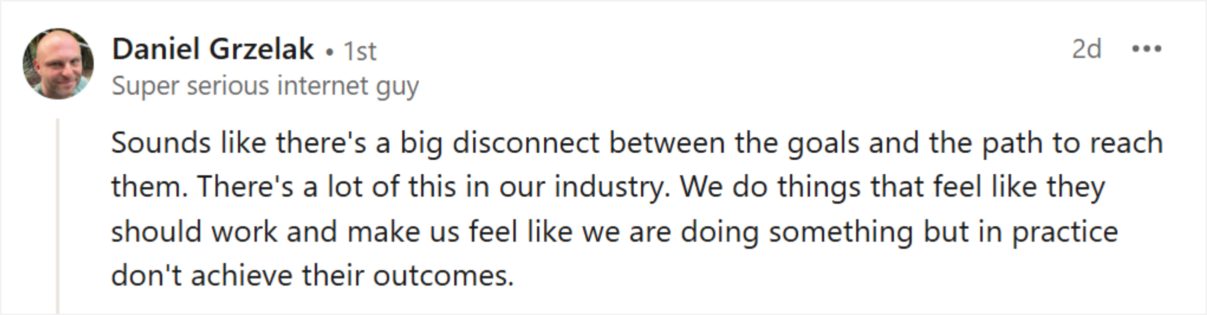
Ian Glover, president of infosec accreditation body CREST, is stepping down from his post, he told the organisation's annual general meeting yesterday.

Sources whispered of Glover's departure to *The Register* ahead of a mass mailout today to members of the organisation, which oversees some industry-recognised penetration testing exams and certifications in the UK.

Source 1 and Source 2

Daniel Grzelak, Chief Innovation Officer at Plerion, ex CISO of Atlassian (20 years of experience)

On the 20th of January 2025, Daniel published this:



Daniel Grzelak • 1st 2d •••

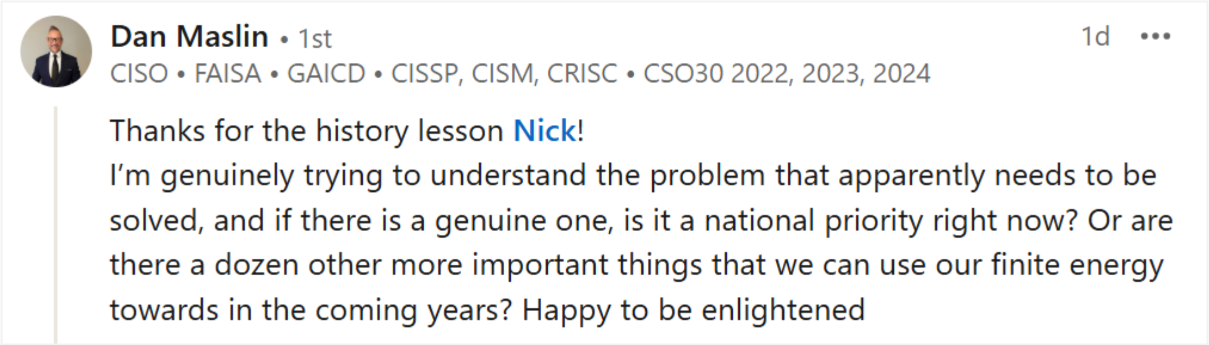
Super serious internet guy

> Sounds like there's a big disconnect between the goals and the path to reach them. There's a lot of this in our industry. We do things that feel like they should work and make us feel like we are doing something but in practice don't achieve their outcomes.

Source

Dan Maslin, Group CISO at Monash University (30 years of experience)

On the 21st of January 2025, Dan published this:



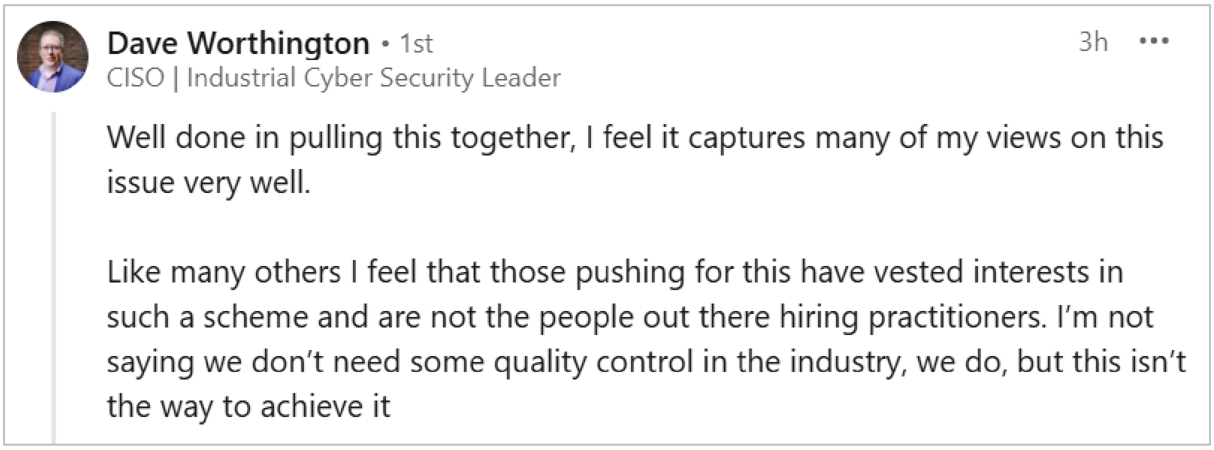
Dan Maslin • 1st
CISO • FAISA • GAICD • CISSP, CISM, CRISC • CSO30 2022, 2023, 2024

Thanks for the history lesson Nick!
I'm genuinely trying to understand the problem that apparently needs to be solved, and if there is a genuine one, is it a national priority right now? Or are there a dozen other more important things that we can use our finite energy towards in the coming years? Happy to be enlightened

Source

Dave Worthington, CISO at Jemena (30 years of experience)

On the 25th of January 2025, Dave published this:



Dave Worthington • 1st
CISO | Industrial Cyber Security Leader

Well done in pulling this together, I feel it captures many of my views on this issue very well.

Like many others I feel that those pushing for this have vested interests in such a scheme and are not the people out there hiring practitioners. I'm not saying we don't need some quality control in the industry, we do, but this isn't the way to achieve it

Source

David Cheal, Chief of All Things, Thermite (15 years of experience)

On January 20th, 2025, David published this:

Recently, I saw a post by Tony Vizza about the need for professional standards / regulation within Cybersecurity. My replies were critical of the idea, and he probably got the impression I didn't think Cybersecurity required regulation or that it wasn't important.

Which isn't actually the case. I think we can and should do a lot to dramatically improve cybersecurity across all Australian businesses, organisations, and government bodies. The frequent news of breaches provides a clear indicator of how shit things are.

The issue isn't about people though, it's about the function of cybersecurity and the economic/regulatory landscape it operates in.

“You can't have Professional people in an industry that isn't Professional.”

Let's ignore for the moment the pros and cons of establishing Cybersecurity as a “Profession”. Assume it's a given, and something very similar to the Australian Computer Society standards for Ethics/Practice is put in place.

First up, who are these cybersecurity people?

When most people think of cybersecurity, they imagine technical people working away behind keyboards to secure technology. This is true to an extent, but there are also many people who came from other disciplines. There is overlap with other functions such as compliance / governance, and you can be in cybersecurity with relatively little technical skills.

There are an awful lot of cybersecurity professionals that have never tried to attack or defend a server. They know the importance of secure password policies, but don't know how to reset their password in Active Directory.

Who are they working for?

Anyone and everyone, from government departments, companies, non-profits, and consultancies. Most of these roles exist in corporations as an internal function or in a consultancy, as few businesses are big enough to need or afford a full-time function.

So what the problem with creating a “Profession”?

To be a held to any standard when you fill a function, you have to establish the following:

Your client/employer must also fall under that standard

Or, at a minimum, can't force you to break the standard

These constraints need to be enforced by legislation

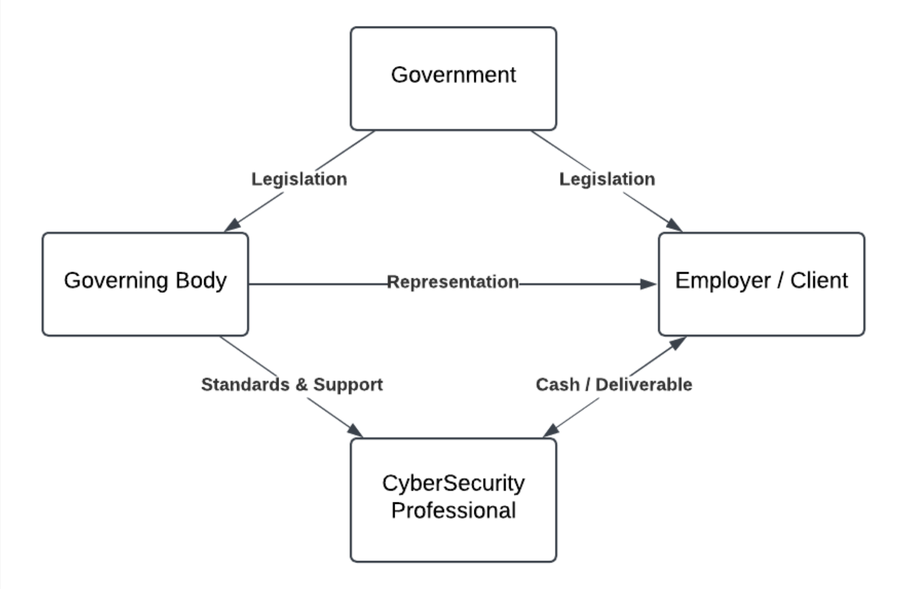
Without that, all you have is a voluntary framework that some people have decided to follow. If you want to establish something like the ACS, set arbitrary rules and say all members must follow them, knock yourself out. Everyone needs a hobby.

But these types of frameworks don't have any teeth in the real world. They won't improve cybersecurity within Australian entities, and it will just be something for the CV. These sorts of standards are just marketing. You can tell it’s just marketing because there’s no list of people who have had their membership revoked.

Real professions, share their blacklist so that people know whom to avoid when hiring. ie

- Law
- Health

If you want cybersecurity professionals to be bound by a rule, they require legislation that obligates them to do so, while also protecting them in its execution. All the professional standards, have to come from the governing body and supporting law, NOT the employer/customer. The client / employer must have nothing to do with establishing standards.



Think about a doctor. You can have confidence a doctor will keep your itchy rash confidential. However, if it turns out you've got a new STI never seen before by science, they will report your case to relevant people.

You can't stop that report from going in, no matter how much you'd rather it didn't. Nor can the med centre the doctor works at. You can't sue the doctor for breach of contract or defamation etc.

To make professionalisation work, you have to establish a governing body that the members must place before the client when it comes to standards. You are hired by someone true, but you are always loyal to the governing body and standards.

Importantly, the client/employer knows that there is little chance of members abandoning those standards and even less chance of compelling them to do so.

Presently, there is no legislation that defines what "Professional" cybersecurity activity/behaviour even looks like. What cybersecurity legislation exists, is typically broad and consists of recommendations or best-practices.

Which is very deliberate because;

- Corporations have absolutely no interest in binding themselves to a series of legally enforceable cybersecurity obligations that are outside their control. It's bad for business.
- Governments have no interest in pissing off business lobby groups or having companies go broke via penalties. It's bad for your election chances.

Ethics

I'm going to skip most of the ethics conversation. Not because I don't think it's important, or interesting, but because it's subjective. Your idea of ethical, is not my ethical. To give a simple example;

Personally, I would never work for, or have a client that provides gambling services. Sure, it's legal and they have a lot of cash. But I'm not an amoral asshole, hellbent on making money from human tragedy and suffering. That's just me.

The ACS Code of Professional Conduct states that ACS members should:

"protect and promote the health and safety of those affected by your work;" 1.2.2.b

Yet, there are ACS members working in the gambling industry. Go figure.

The employer and cybersecurity authority

Employers have zero interest in cybersecurity staff aligning with a legally binding Professional Standard. It is most definitely is not in their commercial interests. Any real increase in IT security has a very material impact on budgets and timelines.

Companies implement IT security based on three things:

- What they are compelled to do under law
- Within those legal obligations, act on cost vs possible penalties
- Self Preservation, based on how hard stakeholders push, and whether decision makers give a fuck

A cybersecurity professional has zero authority to make anything happen, unless given it by the client/employer. They exist to identify, report and remediate as directed. Nothing more. The CISO can't override a CEO.

Why this Profession, is just a profession

Let's look at a real-world challenge.

- You are auditing systems and notice that the production internet facing servers haven't been patched in over 3 years. They are exposed to multiple CVE's that are actively being exploited in the wild. If they are breached, tens of thousands of customer PII records will be exposed. But no sign of a breach so far!
- You notify leadership, who says that it's a known thing, but there is no time or budget allocated, so they are not going to patch them. It's SOP at the business to kick patching down the road.

What's a Cybersecurity Professional to do?

In the ACS code, it states that:

- "In your work, you should safeguard the interests of your immediate stakeholders, provided that these interests do not conflict with the duty and loyalty you owe to the public" (The Primacy of the Public Interest 1.2.1)
- "advise your stakeholders as soon as possible of any conflicts of interest or conscientious objections that you have;" (The Primacy of the Public Interest 1.2.1.b)
- "Not remain silent when you detect unprofessional conduct." (Honesty 2.1.a)

It would clearly be unethical to simply ignore this situation. Before you throw yourself on your sword though, let's check the companies position. Surely, the Australian Privacy Act 1988 has your back right?

Yeah, not so much. The Privacy act has 448 pages, but you won't find "you must patch servers" in the legislation. You will find this item in "APP 11 Security of personal information":

"An APP entity that holds personal information must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure "

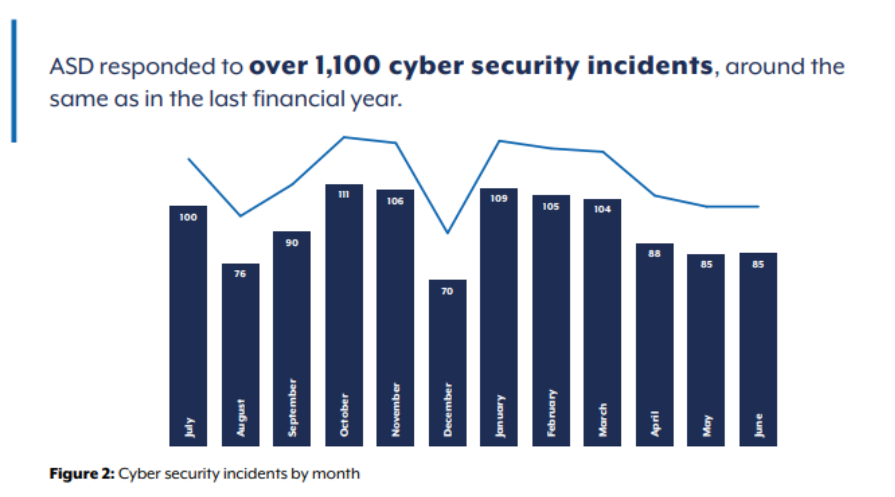
Unfortunately, this isn't as helpful as you might think. The key word here is "reasonable".

Reasonable is very much up for debate and takes an awful lot of things into consideration. The cybersecurity professional, public, company, and courts are all going to have very different ideas of what "reasonable" means. In this case, the company will say that patching the servers is very unreasonable for a long list of reasons. One being "Fuck you, I hired you to fix my shit not give me grief about patching servers."

In the end, the big problem is commercial risk vs reward. The company has been running the gauntlet so far, and cant see a reason to change. They have put the servers in the risk register, and it's flagged for discussion in next quarter's budget. In the interim, they are willing to take the risk of a hack.

Even if they get hacked, the likelihood of the OAIC taking them to court is very low. The chance of a fine is astronomically small.

The ASD responded to some 1100 incidents in 2024, so breaches are pretty common.



ASD responded to **over 1,100 cyber security incidents**, around the same as in the last financial year.

Figure 2: Cyber security incidents by month

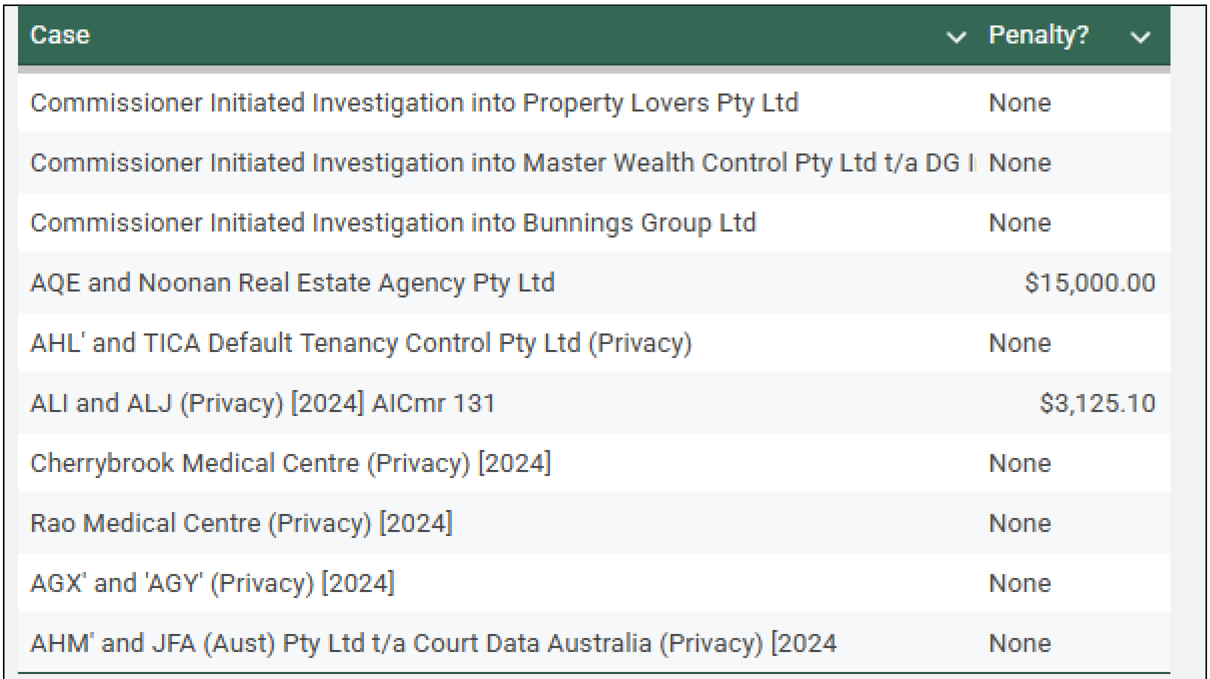
Surely, the OAIC found some of these companies had breached the Privacy Act and punished them? Lets check:

Enforceable Undertakings: 2

Inspiring Vacations: 100k records exposed via S3 bucket, but they promised to do better. No fine.

Meta: The Cambridge Analytica mess. Meta promised not to do it again and paid $50M in penalty. Which sounds like a lot, until you realise it's less than 1% of Australian annual revenue, and only slightly more than Zuck spends on shoes.

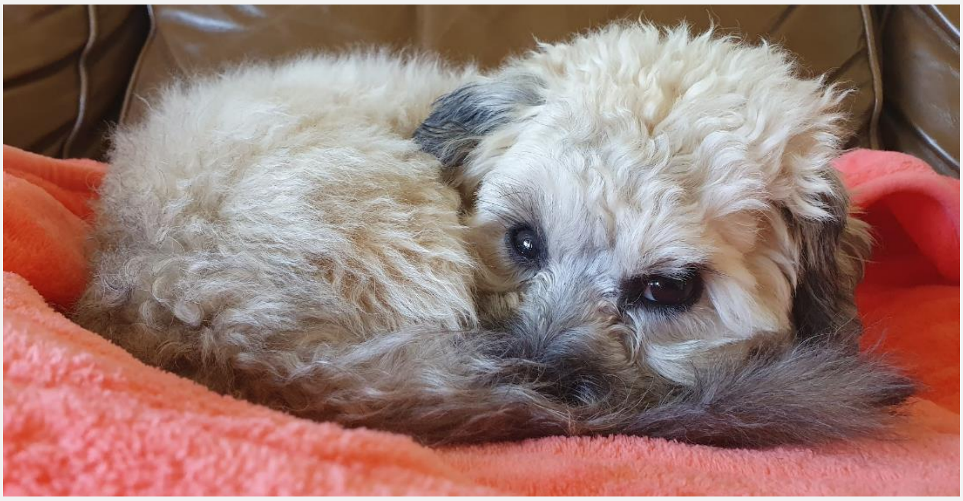
Court Cases: 10



Case	Penalty?
Commissioner Initiated Investigation into Property Lovers Pty Ltd	None
Commissioner Initiated Investigation into Master Wealth Control Pty Ltd t/a DG I	None
Commissioner Initiated Investigation into Bunnings Group Ltd	None
AQE and Noonan Real Estate Agency Pty Ltd	$15,000.00
AHL' and TICA Default Tenancy Control Pty Ltd (Privacy)	None
ALI and ALJ (Privacy) [2024] AICmr 131	$3,125.10
Cherrybrook Medical Centre (Privacy) [2024]	None
Rao Medical Centre (Privacy) [2024]	None
AGX' and 'AGY' (Privacy) [2024]	None
AHM' and JFA (Aust) Pty Ltd t/a Court Data Australia (Privacy) [2024	None

Of the ten court cases I could find in relation to the Australian Privacy Act, all got found guilty of a breach. Only 2 got fines (the ten cents is amusing).

The message is clear, companies really don't give have to care about the OAIC and the Australian Privacy Act. My pet Chihuahua x poodle cross has more bite.



So where does that leave our ethical Cybersecurity Professional?

- The governing body standards are clear, working on this project would be unethical.
- The employer has listened to, and dismissed the request to patch
- The employer isn't going to resolve the issue and has no legal obligation to patch.
- They have no fear of the OAIC, should they be breached.

You could leak the information. If you're very lucky, there is a whistleblower clause in your contract to avoid the NDA you undoubtably signed. Either way, you can kiss your career goodbye in that company.

If word gets out you leak, you can forget finding another gig in cyber. You sure as fuck won't be working for a cybersecurity consultancy. An ex hacker/criminal is one thing, but nobody will touch a corporate snitch.

> You can quit, but the rent won't pay itself. Have fun explaining to your family why the bills are overdue because you prioritised server patching.
>
> Now I'm just some uneducated, uncertified, unprofessional tech guy; but how’s this professionalism thing meant to work again?
>
> **PS**
>
> One last thing, if you’re an advocate for cybersecurity and professionalism, I think it's a good idea to practice what you preach. There are 11 members of the ACS Technical Advisory Board, 4 make up the cybersecurity board. Each with LinkedIn profiles pointing to their respective websites.
>
> That includes:
>
> - Link pointing to an expired domain with dropcatch. Domain hijack waiting to happen.
> - A self-hosted WordPress server that is 6 minor releases behind, that runs on a VPS that is also an SMTP, POP3 and DNS server
> - A self-hosted WordPress site on VPS that is also an FTP, DNS, SMTP, POP3 server
> - A self-hosted IIS server on VPS that is also an FTP server
> - A self-hosted WordPress that is also an SMTP, POP3, DNS and FTP server
> - Website on VPS that is also an FTP, SMTP, DNS, and DB server (with DB connection open to the internet)
> - Self hosted WordPress on VPS that is also an FTP, DNS, SMTP server
> - Site down, expired domain
>
> THE END

Source: https://www.linkedin.com/pulse/you-cant-professional-unprofessional-industry-david-cheal-kmysc/

Dale J. Consultant, ex Chief Security Architect for the ATO (20 years of experience)

On the 25th of January 2025, Dale published this:

> Doctor botched a surgery? Lawyer gave you bad advice? Practicing certificate revoked, sued into oblivion.
>
> CISO campaigns against security standards? Boards under fund security measures? Lawyers abuse professional legal privilege to prevent recovery? Zero tangible consequences to date.
>
> Cyber security won't be a certifiable profession before we are charging $600 per hour, held personally liable for poor advice, hold professional indemnity insurance at a cost exceeding $20,000 per annum and CISOs/board members are held criminally liable for reckless and negligent security decisions.
>
> If you want to certify a body of talent as a profession, treat it like one. I'm personally comfortable with that outcome, but absent the very costly framework, I can't support it.

Source

Edward Farrell, CEO at Mercury Information Security Services (20 years of experience)

On the 20th of January 2025, Ed published this:

> If you ever need good cause as to why cyber security as an industry should have professionalisation commensurate to doctors, engineers, accountants and nurses I would suggest you have a good read of "WUT v Victoria Police [2020] VSC 586." This was an individual with a cyber business that also doubled up as a private investigator whose overstated cyber security claims and professional conduct at least saw their licence as a private investigator suspended, but as a cyber security practitioner remained in business and saw them fleece tens of thousands of dollars out of desperate Australians dealing with domestic violence, ransomware and a myriad of other unfortunate events.
>
> I have sought to hold myself and colleagues to a high degree of accountability, weather its vapourware firewalls or another overpriced copypasta Nessus report, there is a need to provide a set of guidelines so that we can operate against an agreed baseline, and deal with those who refuse to do so. Thankfully, the government is here to help:
>
> https://www.grants.gov.au/Go/Show?GoUuid=42ef2485-3b41-4583-9003-c5b562f0b528
>
> Whilst I welcome the $1.9 million in funding to design, promote and pilot a professionalisation scheme for Australia's cyber security workforce, the open natured tender of this as well as the previous cybersecurity ministers fixation on style over substance leaves me concerned as to the nature and intent of this program on the verge of an election. Factor in that the very needs of the scheme, to tackle unprofessional conduct, first needs to overcome the risk that said conduct could inadvertently transcend into such a scheme.
>
> Haphazardly rushed before the Government goes into caretaker mode, There are half a dozen ways I can see this scheme failing:
>
> 1) A single overseeing entity for the scheme with a reputation of gatekeeping is awarded the scheme development, requiring overpriced association fees in order for people to generate a living.
> 2) A training and education provider, weather its a university, TAFE or "we make cyber geniuses in 6 months academy" defines professional standards requiring attendance on their training course, thereby making entry of competitors prohibitive or difficult, also contributing the the monopolisation and destroying innovation.
> 3) A "big 4 consulting" pyramid scheme wins the contract and throws 23 year old know it all's on hourly billing rates, leading to a cost overrun, a weak scheme and a firm partner getting a bit of extra cash to blow at the ivy pool bar.
> 4) The standards are "uniquely Australian" because a genius decided to "roll their own" bespoke hand crafted scheme, and as a result skills transference and harmonisation with best practice does not take place, because someone had to be special, leading to increased operational costs in the schemes sustainment.
> 5) Egos (including my own) fracturing any cohesion or logical thought in structuring a professional scheme.
> 6) Divine ministerial intervention awarding it to the highest bidder (via election donations).
> 7) Any not for profit association that is rightfully awarded the scheme has their board highjacked in the near future by a pack of vultures looking to commercially exploit the scheme for their own benefit.
>
> Essential to this scheme will be:
>
> 1) Enfranchisement: as a practitioner, I want to be onboard. I also want domains that do not require

technical rigour to be apart of such as scheme as their actions also have an impact and require some form of conduct.

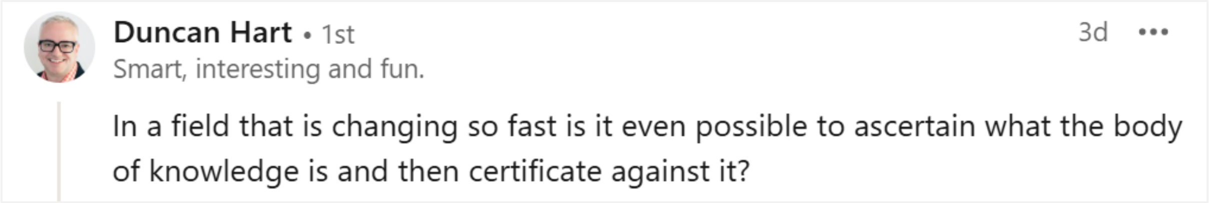
2) Collaboration: multiple associations and industry bodies have a say in this scheme and have already done most of the work.
3) Harmonisation: the UK has a great scheme in place. Whilst university frowns on plagiarism, success in this domain does not.
4) Building on what's already been done. Tony Vizza and Jill Slay have already conducted prepared research on this topic which is excellent. Once again, we do not need to reinvent the wheel.

I am hopeful that whoever takes on this task is aware of the need for professionalisation, but also conscious of the harm which ill-tempered good intentions can lead to. Let hope cool minds prevail in the schemes selector, implementer and contributors.

Source: https://www.linkedin.com/pulse/how-stuff-up-impending-cyber-industry-edward-farrell-f9ltc/

Duncan Hart, Managing Partner at RiskQuant (15 years of experience)

On the 20th of January 2025, Duncan published this:



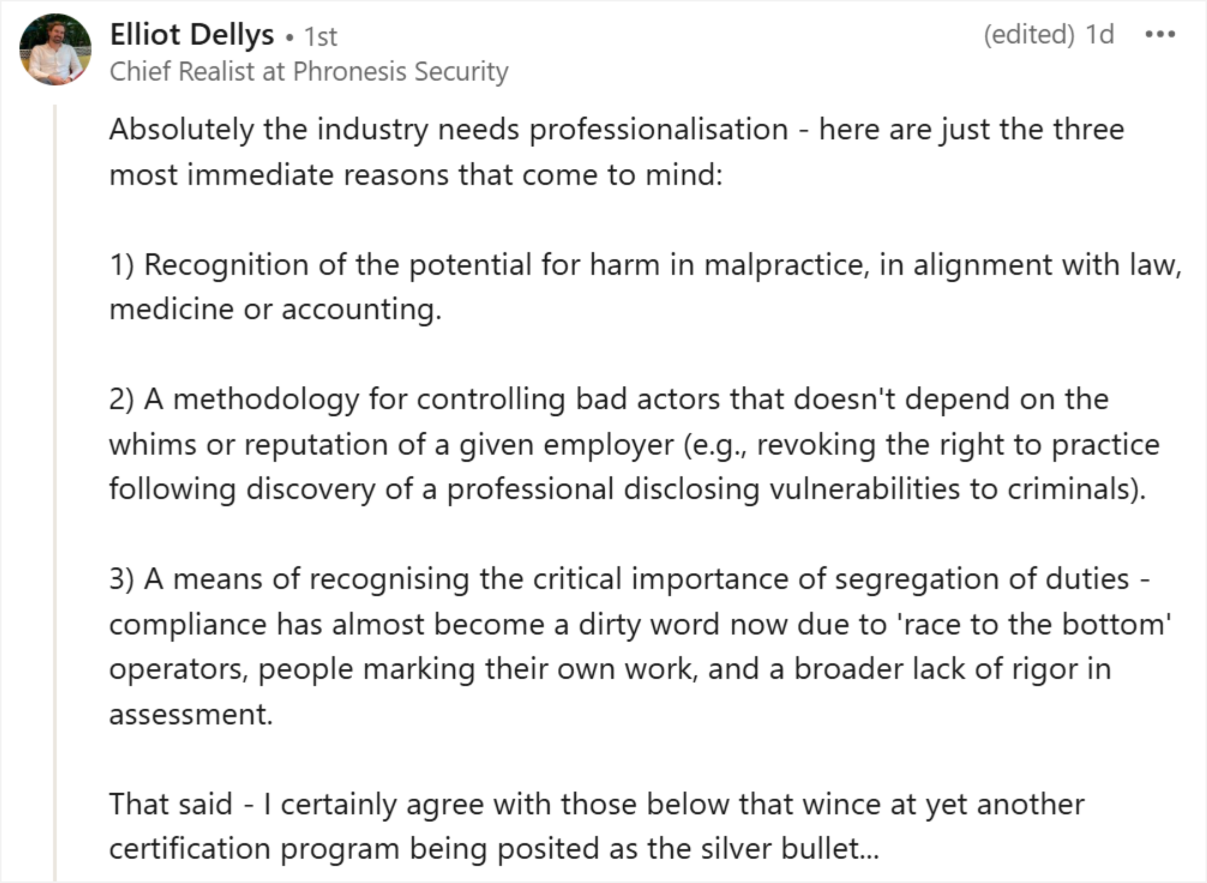
Duncan Hart • 1st 3d •••
Smart, interesting and fun.

In a field that is changing so fast is it even possible to ascertain what the body of knowledge is and then certificate against it?

Source

Elliot Dellys, Chief Realist at Phronesis Security (15 years of experience)

On the 21st of January 2025, Elliot published this:



Elliot Dellys • 1st (edited) 1d

Chief Realist at Phronesis Security

Absolutely the industry needs professionalisation - here are just the three most immediate reasons that come to mind:

1) Recognition of the potential for harm in malpractice, in alignment with law, medicine or accounting.

2) A methodology for controlling bad actors that doesn't depend on the whims or reputation of a given employer (e.g., revoking the right to practice following discovery of a professional disclosing vulnerabilities to criminals).

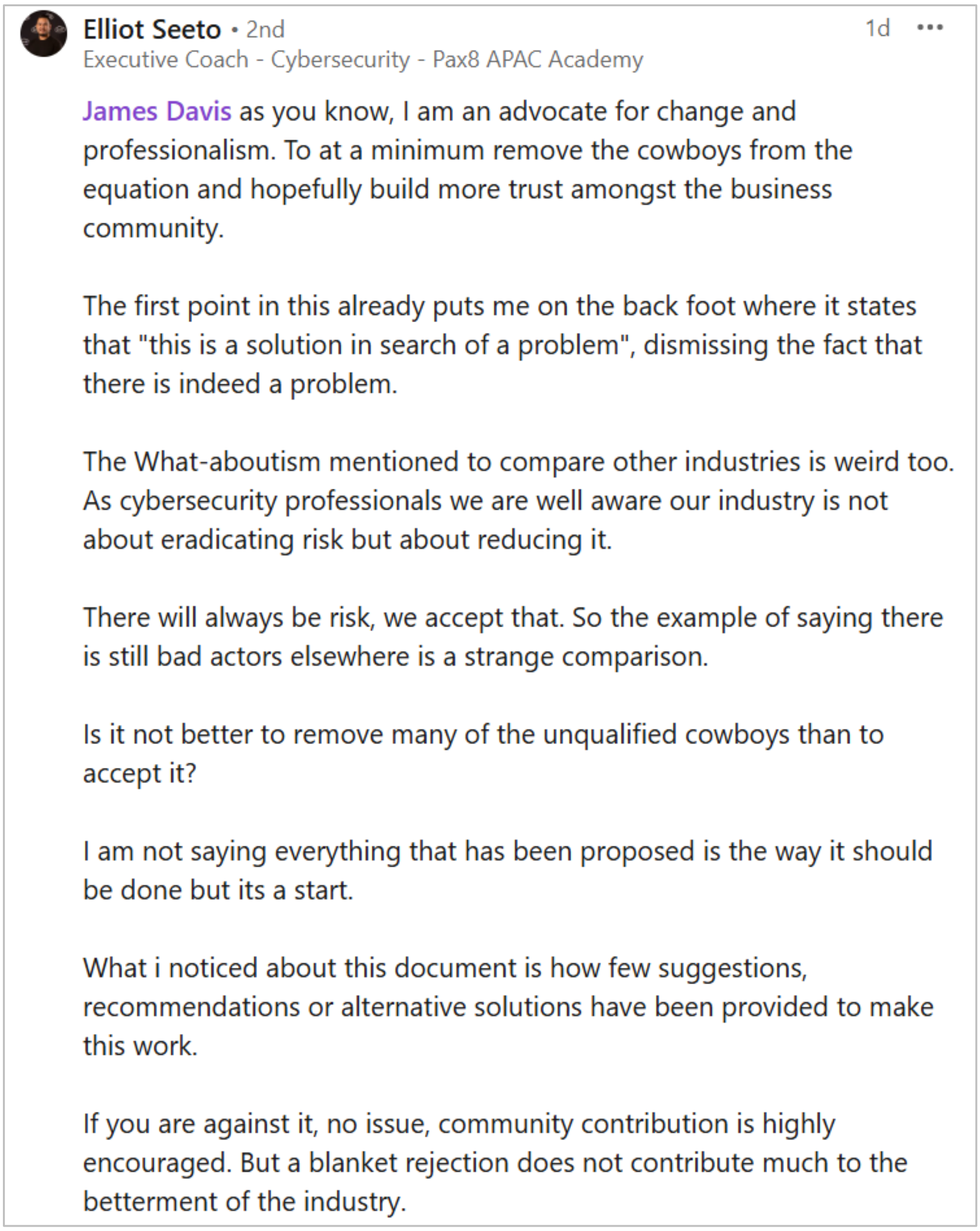
3) A means of recognising the critical importance of segregation of duties - compliance has almost become a dirty word now due to 'race to the bottom' operators, people marking their own work, and a broader lack of rigor in assessment.

That said - I certainly agree with those below that wince at yet another certification program being posited as the silver bullet...

Source

Elliot Seeto, Executive Coach at Pax8 (15 years of experience)

On the 24th of January 2025, Elliot published this:



Elliot Seeto • 2nd
Executive Coach - Cybersecurity - Pax8 APAC Academy

James Davis as you know, I am an advocate for change and professionalism. To at a minimum remove the cowboys from the equation and hopefully build more trust amongst the business community.

The first point in this already puts me on the back foot where it states that "this is a solution in search of a problem", dismissing the fact that there is indeed a problem.

The What-aboutism mentioned to compare other industries is weird too. As cybersecurity professionals we are well aware our industry is not about eradicating risk but about reducing it.

There will always be risk, we accept that. So the example of saying there is still bad actors elsewhere is a strange comparison.

Is it not better to remove many of the unqualified cowboys than to accept it?

I am not saying everything that has been proposed is the way it should be done but its a start.

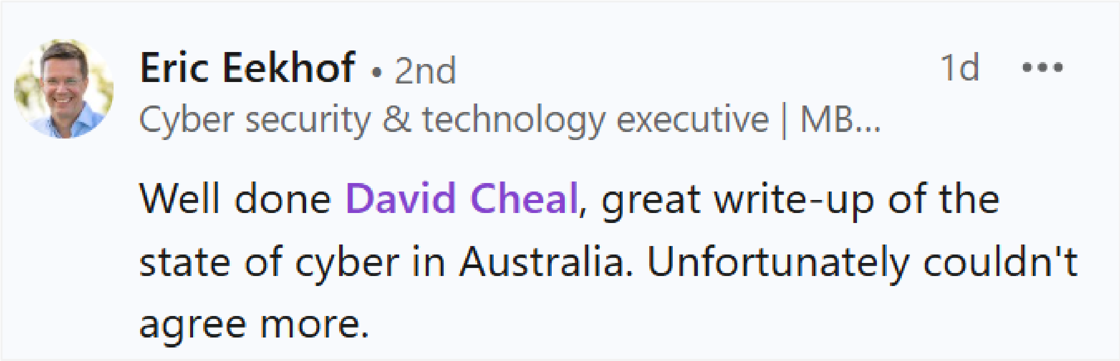
What i noticed about this document is how few suggestions, recommendations or alternative solutions have been provided to make this work.

If you are against it, no issue, community contribution is highly encouraged. But a blanket rejection does not contribute much to the betterment of the industry.

Source

Eric Eekhof, Principal Security Architect at Astralas (20 years of experience)

On the 22nd of January 2025, Eric published this:



Eric Eekhof • 2nd 1d •••

Cyber security & technology executive | MB...

Well done David Cheal, great write-up of the state of cyber in Australia. Unfortunately couldn't agree more.

Source

Eric Pinkerton, Director NSW at Phronesis Security (20 years of experience)

On January 22nd, 2025, Eric published this:

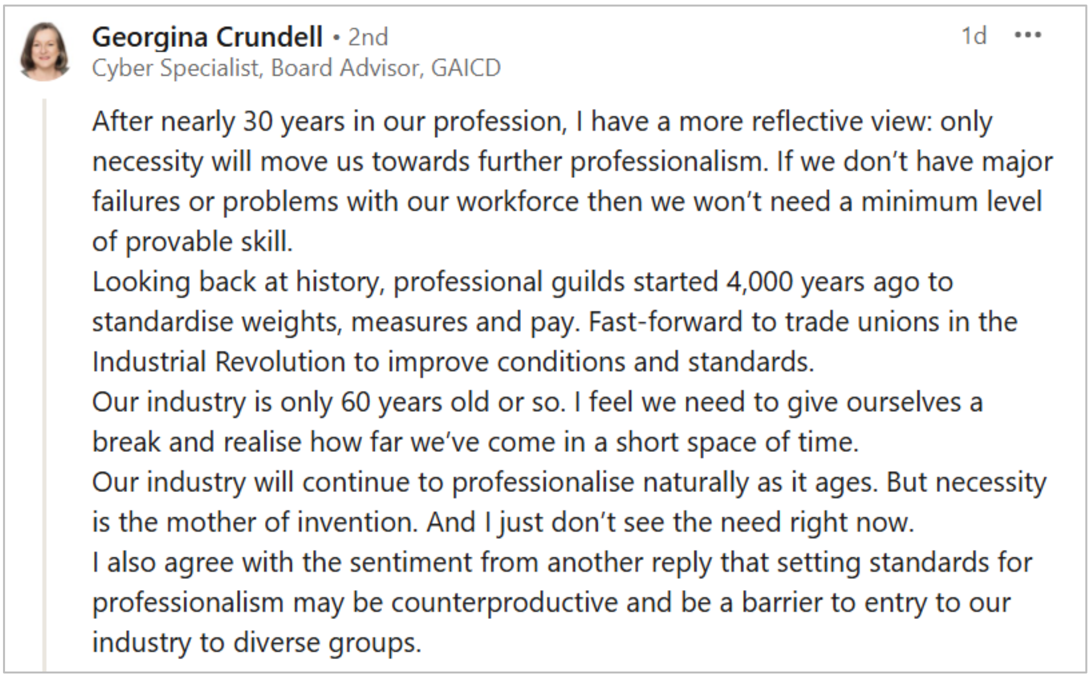
> With all the AI Generated BotS#$t and endless debate about the intent of Elon's salute etc on here, it's been really great to see some good old fashioned home grown cyberdrama play out around the proposed Professional Recognition Scheme for the Australian Cyber Security Profession. I think the fact people are impassioned about this is a really healthy sign.
>
> I really like Tony Vizza and Jill S.' Whitepaper on this and think it's a good starting point, and I also share Nick Ellsmore's cynicism (I have learned over time that Nick is very rarely wrong about anything cyber). I also find Edward Farrell's concerns pretty compelling.
>
> It's pretty clear to me that the status quo isn't cutting it, and we need to move forward at some point, before we inevitably befall a series of 'compelling events' that will reflect badly on our industry as a whole. I assume many people died before the medical profession got it's house in order, and I say this despite feeling that a lot of the rhetoric about Cybersecurity being 'life and death' is still for the most part hyperbole and so probably unhelpful in this debate.
>
> A pervasive claim that is hard to decouple from this discussion, and one which I vehemently disagree with is that this industry is struggling to fill hundreds of unfilled roles.
>
> There are certainly open roles in the cybersecurity field, but the challenge often lies in aligning expectations between employers and candidates. Some organisations may seek highly experienced professionals for entry-level positions or offer salaries that don't reflect the required skillset. This can create the impression of a widespread skills shortage, when in fact, it's more a matter of market dynamics.
>
> Furthermore, the way vacancies are advertised can inflate the perceived number of open roles. A single position might be posted across multiple platforms and re-advertised frequently, creating the illusion of numerous unfilled positions that simply don't exist.
>
> The narrative of a massive skills gap can be misleading and in my view is mostly influenced by organisations that benefit from perpetuating this perception such as training providers selling the dream of landing a well paid job role after completing a short bootcamp, and then of course there is the ACS who profit directly from number of people overseas pursuing the dream of skilled migration at a time when the

> government is implementing immigration caps.
>
> I acknowledge that some sort of professional licencing scheme is something that is probably overdue, and also that it throws up some really wicked problems to solve. These compound the risk of it resulting in a cobra effect, most notably the opportunities for the organisation that will become the governing body to mismanage it somehow.
>
> To do it properly we will need to establish a Quango to provide the oversight, and to that point, making sure it's not a Training Provider, or the ACS is the hill I am most prepared to die on!

Source: https://www.linkedin.com/pulse/good-old-fashioned-cyber-drama-eric-pinkerton-bnlxc/

Georgina Crundell, Board Advisor at Australian Retirement Trust, ex EY Partner (30 years of experience)

On the 24th of January 2025, Georgina published this:



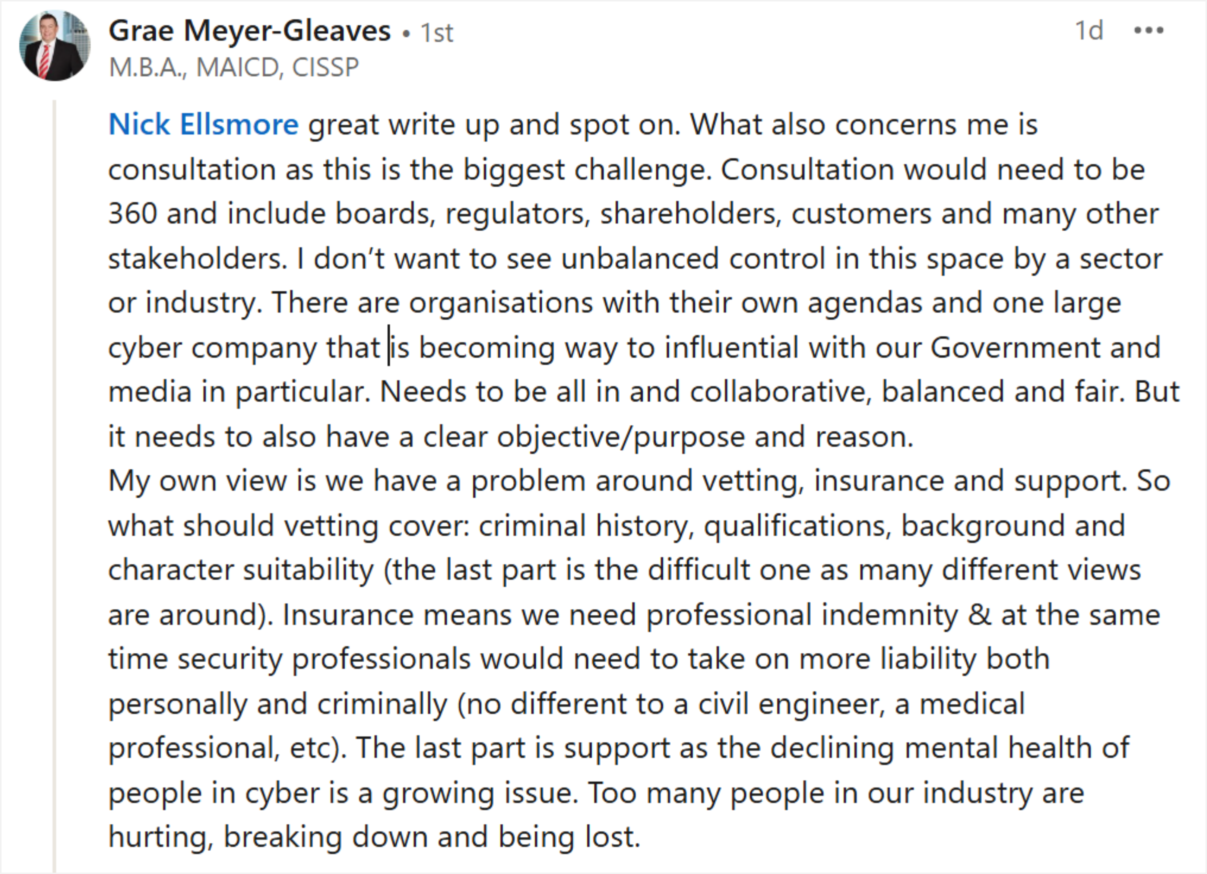
Georgina Crundell • 2nd
Cyber Specialist, Board Advisor, GAICD
1d •••

After nearly 30 years in our profession, I have a more reflective view: only necessity will move us towards further professionalism. If we don't have major failures or problems with our workforce then we won't need a minimum level of provable skill.
Looking back at history, professional guilds started 4,000 years ago to standardise weights, measures and pay. Fast-forward to trade unions in the Industrial Revolution to improve conditions and standards.
Our industry is only 60 years old or so. I feel we need to give ourselves a break and realise how far we've come in a short space of time.
Our industry will continue to professionalise naturally as it ages. But necessity is the mother of invention. And I just don't see the need right now.
I also agree with the sentiment from another reply that setting standards for professionalism may be counterproductive and be a barrier to entry to our industry to diverse groups.

Source

Grae Meyer-Gleaves, Information Security Leader at Cubic Transportation Systems (30 years of experience)

On the 21st of January 2025, Grae published this:



Grae Meyer-Gleaves • 1st
M.B.A., MAICD, CISSP

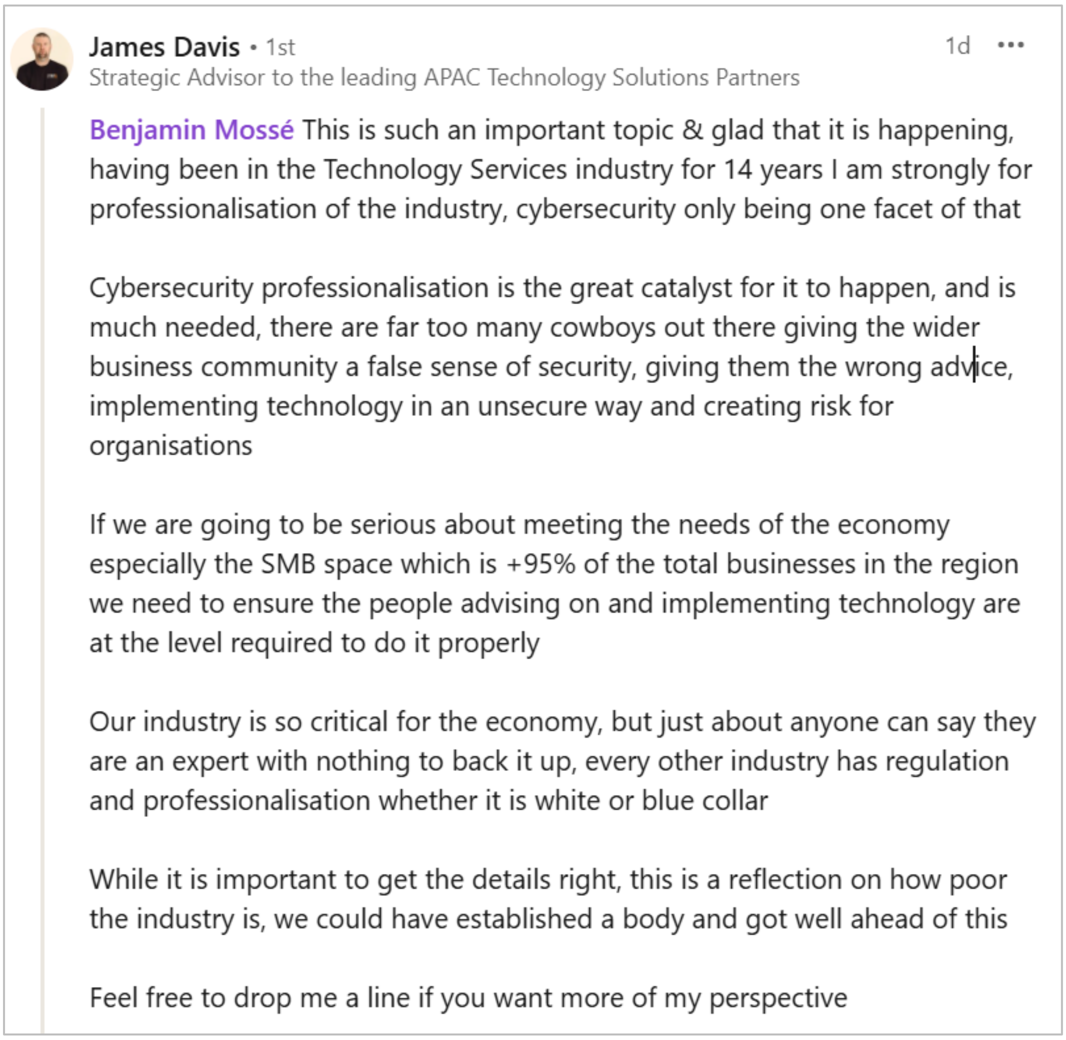
1d •••

Nick Ellsmore great write up and spot on. What also concerns me is consultation as this is the biggest challenge. Consultation would need to be 360 and include boards, regulators, shareholders, customers and many other stakeholders. I don't want to see unbalanced control in this space by a sector or industry. There are organisations with their own agendas and one large cyber company that is becoming way to influential with our Government and media in particular. Needs to be all in and collaborative, balanced and fair. But it needs to also have a clear objective/purpose and reason.
My own view is we have a problem around vetting, insurance and support. So what should vetting cover: criminal history, qualifications, background and character suitability (the last part is the difficult one as many different views are around). Insurance means we need professional indemnity & at the same time security professionals would need to take on more liability both personally and criminally (no different to a civil engineer, a medical professional, etc). The last part is support as the declining mental health of people in cyber is a growing issue. Too many people in our industry are hurting, breaking down and being lost.

Source

James Davis, Director of Academy APAC at Pax8 (14 years of experience)

On the 24th of January 2025, James published this:



James Davis • 1st 1d •••
Strategic Advisor to the leading APAC Technology Solutions Partners

Benjamin Mossé This is such an important topic & glad that it is happening, having been in the Technology Services industry for 14 years I am strongly for professionalisation of the industry, cybersecurity only being one facet of that

Cybersecurity professionalisation is the great catalyst for it to happen, and is much needed, there are far too many cowboys out there giving the wider business community a false sense of security, giving them the wrong advice, implementing technology in an unsecure way and creating risk for organisations

If we are going to be serious about meeting the needs of the economy especially the SMB space which is +95% of the total businesses in the region we need to ensure the people advising on and implementing technology are at the level required to do it properly

Our industry is so critical for the economy, but just about anyone can say they are an expert with nothing to back it up, every other industry has regulation and professionalisation whether it is white or blue collar

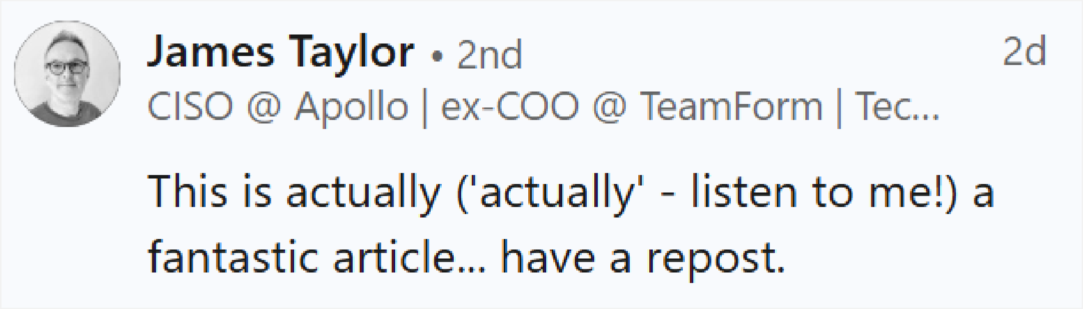
While it is important to get the details right, this is a reflection on how poor the industry is, we could have established a body and got well ahead of this

Feel free to drop me a line if you want more of my perspective

Source

James Taylor, CISO at Apollo (30 years of experience)

On the 22nd of January 2025, James posted this:



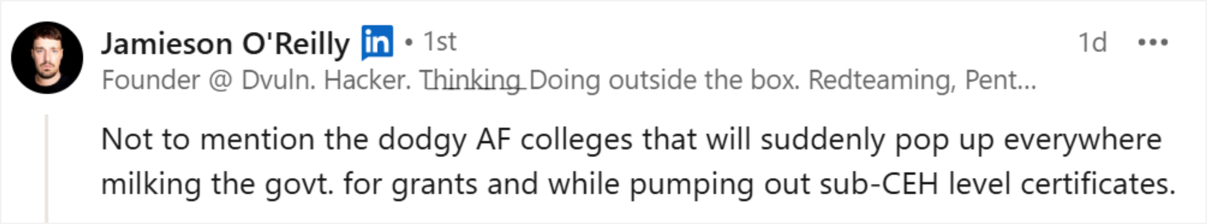
James Taylor • 2nd 2d
CISO @ Apollo | ex-COO @ TeamForm | Tec...

This is actually ('actually' - listen to me!) a fantastic article... have a repost.

Source

Jamieson O’Reilly, Founder at DVULN (12 years of experience)

On the 21st of January 2025, Jamieson published this:



Jamieson O'Reilly • 1st 1d •••

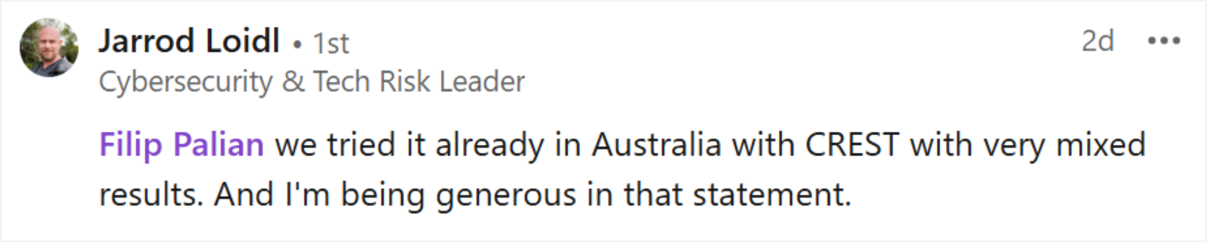
Founder @ Dvuln. Hacker. ~~Thinking~~ Doing outside the box. Redteaming, Pent...

Not to mention the dodgy AF colleges that will suddenly pop up everywhere milking the govt. for grants and while pumping out sub-CEH level certificates.

Source

Jarrod Loidl, Director Deloitte, Board Member EFA (20 years of experience)

On the 20th of January 2025, Jarrod published this:

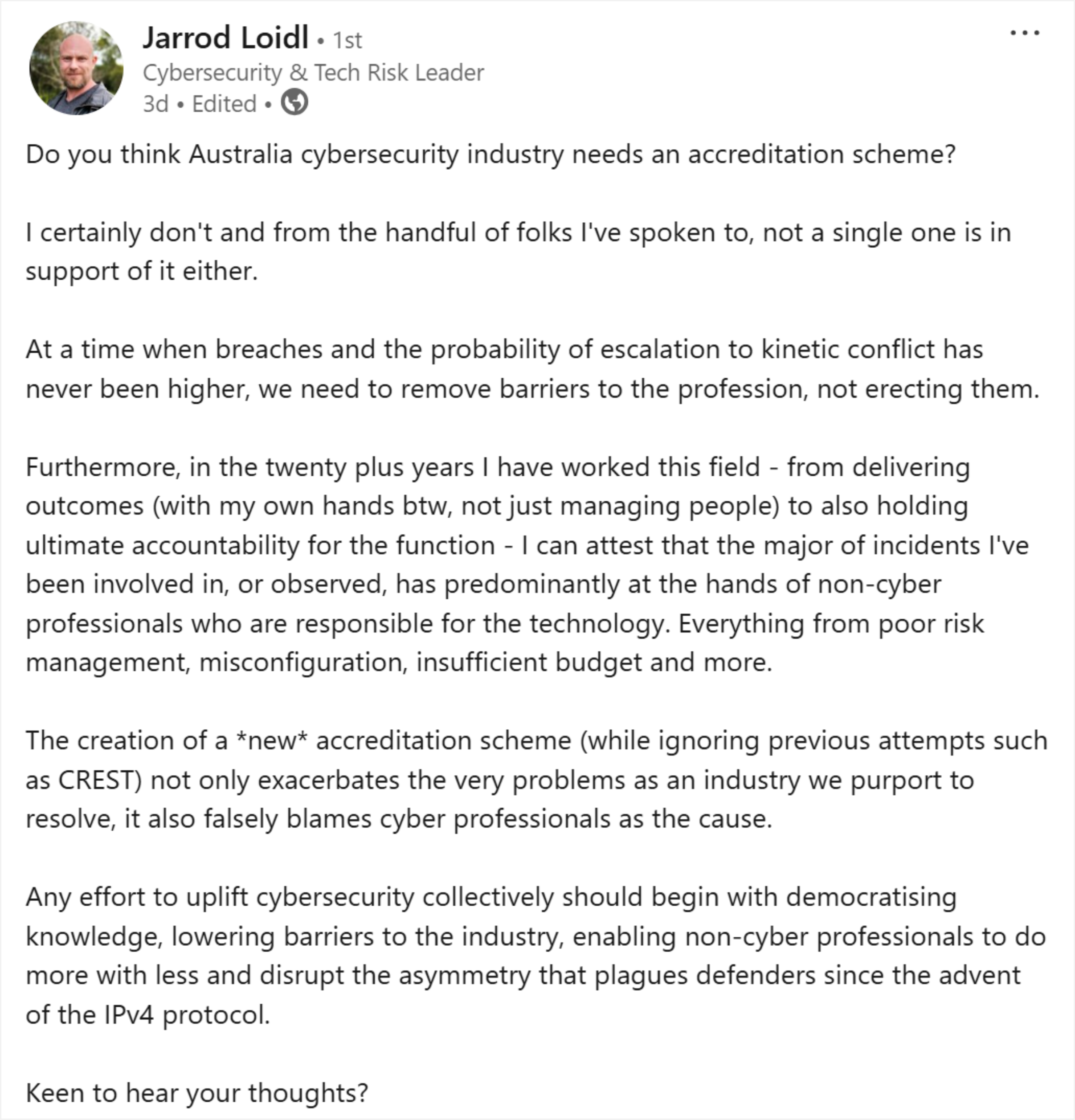


Jarrod Loidl • 1st 2d •••

Cybersecurity & Tech Risk Leader

Filip Palian we tried it already in Australia with CREST with very mixed results. And I'm being generous in that statement.

He also published this:



Jarrod Loidl • 1st
Cybersecurity & Tech Risk Leader
3d • Edited •

Do you think Australia cybersecurity industry needs an accreditation scheme?

I certainly don't and from the handful of folks I've spoken to, not a single one is in support of it either.

At a time when breaches and the probability of escalation to kinetic conflict has never been higher, we need to remove barriers to the profession, not erecting them.

Furthermore, in the twenty plus years I have worked this field - from delivering outcomes (with my own hands btw, not just managing people) to also holding ultimate accountability for the function - I can attest that the major of incidents I've been involved in, or observed, has predominantly at the hands of non-cyber professionals who are responsible for the technology. Everything from poor risk management, misconfiguration, insufficient budget and more.

The creation of a *new* accreditation scheme (while ignoring previous attempts such as CREST) not only exacerbates the very problems as an industry we purport to resolve, it also falsely blames cyber professionals as the cause.

Any effort to uplift cybersecurity collectively should begin with democratising knowledge, lowering barriers to the industry, enabling non-cyber professionals to do more with less and disrupt the asymmetry that plagues defenders since the advent of the IPv4 protocol.

Keen to hear your thoughts?

Source

John Ellis, Global Head of Security at QBE, ex CISO at Bupa (30 years of experience)

On the 25th of January 2025, John published this:

Benjamin, great document you've put together, it raises excellent points. I also appreciate the balance provided by including rebuttals.

Jarriod Loidl, in my view, raises the core question: how does a professionalisation scheme solve the real challenge of making Australian businesses more secure? As he rightly notes, many incidents stem from non-cyber professionals mismanaging technology — through poor risk management, misconfigurations, conflicting priorities, and insufficient budgets.

While professionalisation might help early-career professionals navigate their careers and gain legitimacy, I remain cautious. Secure outcomes depend on solving root causes like mismanagement and underinvestment — areas where professionalisation has limited impact.

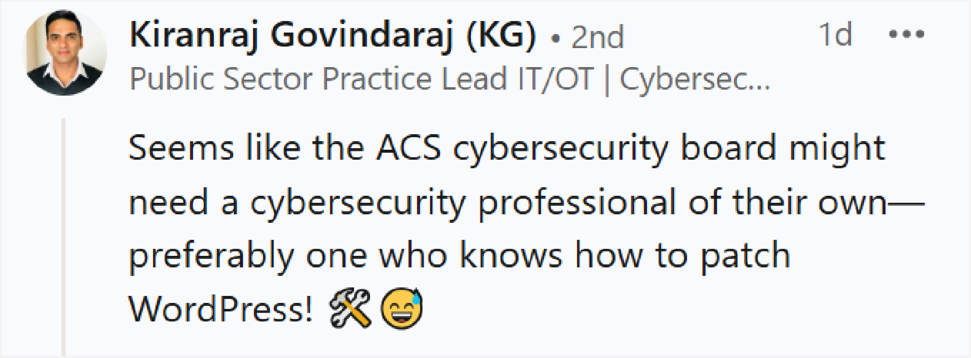
The heart of cyber security lies in people: their curiosity, adaptability, and commitment to learning. Using myself as an example, as I progressed into senior roles, broadening my skills through AICD and board service helped me align with understanding my stakeholder and their needs. Any professionalisation scheme must follow this principle — serving both the profession and those who rely on us.

As a profession, we need to focus on solving the real challenges. Is this one of them?

Source

Kiranraj Govindaraj, Govt / Critical Infrastructure Lead at Darktrace (15 years of experience)

On the 22nd of January 2025, Kiranraj published this:



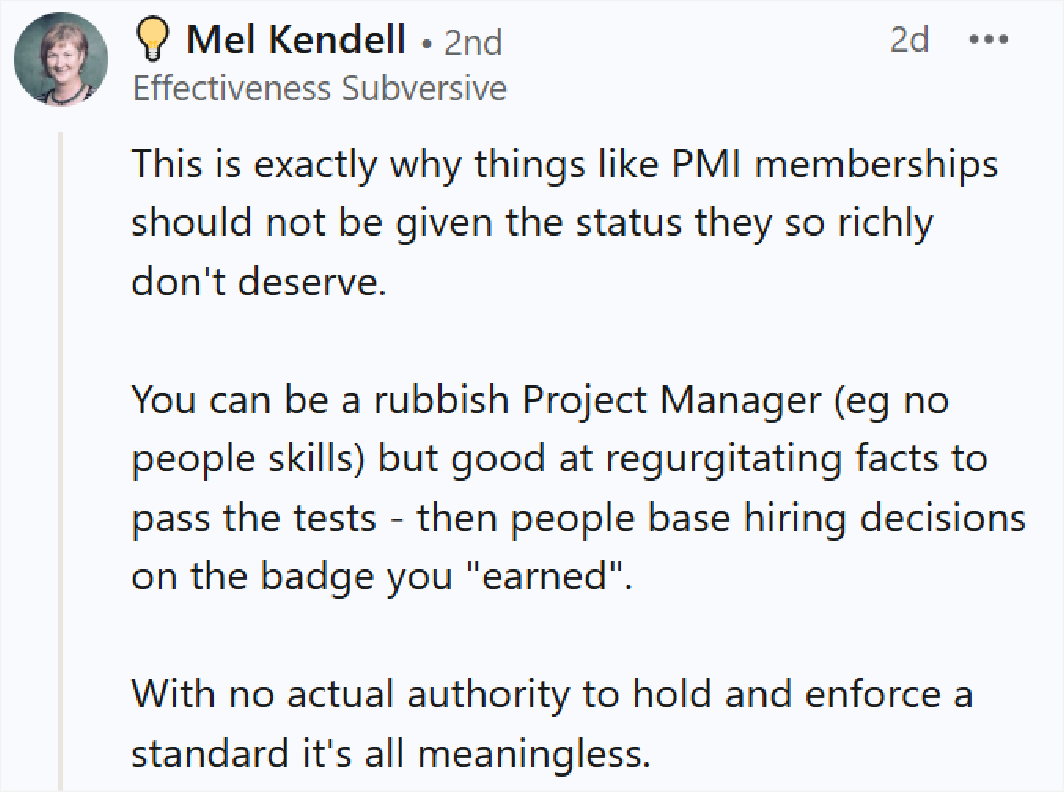
Kiranraj Govindaraj (KG) • 2nd 1d •••
Public Sector Practice Lead IT/OT | Cybersec...

Seems like the ACS cybersecurity board might need a cybersecurity professional of their own— preferably one who knows how to patch WordPress! 🛠️😅

Source

Mel Kendell, Customer Success Consultant at TeamForm (20 years of experience)

On the 21st of January 2025, Mel published this:



Mel Kendell • 2nd 2d •••
Effectiveness Subversive

This is exactly why things like PMI memberships should not be given the status they so richly don't deserve.

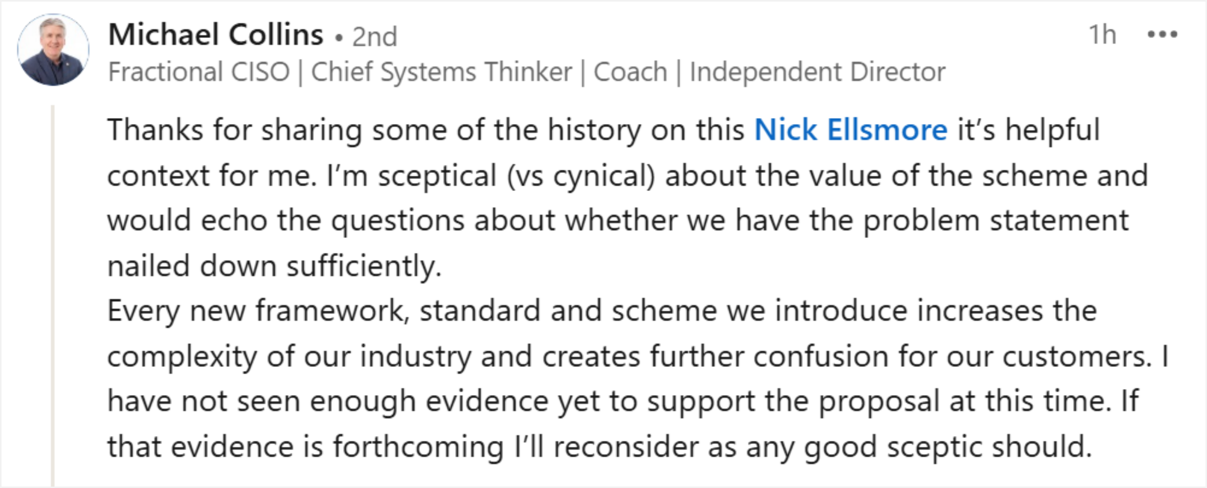
You can be a rubbish Project Manager (eg no people skills) but good at regurgitating facts to pass the tests - then people base hiring decisions on the badge you "earned".

With no actual authority to hold and enforce a standard it's all meaningless.

Source

Michael Collins, Fractional CISO (20 years of experience)

On the 23rd of January 2025, Michael published this:



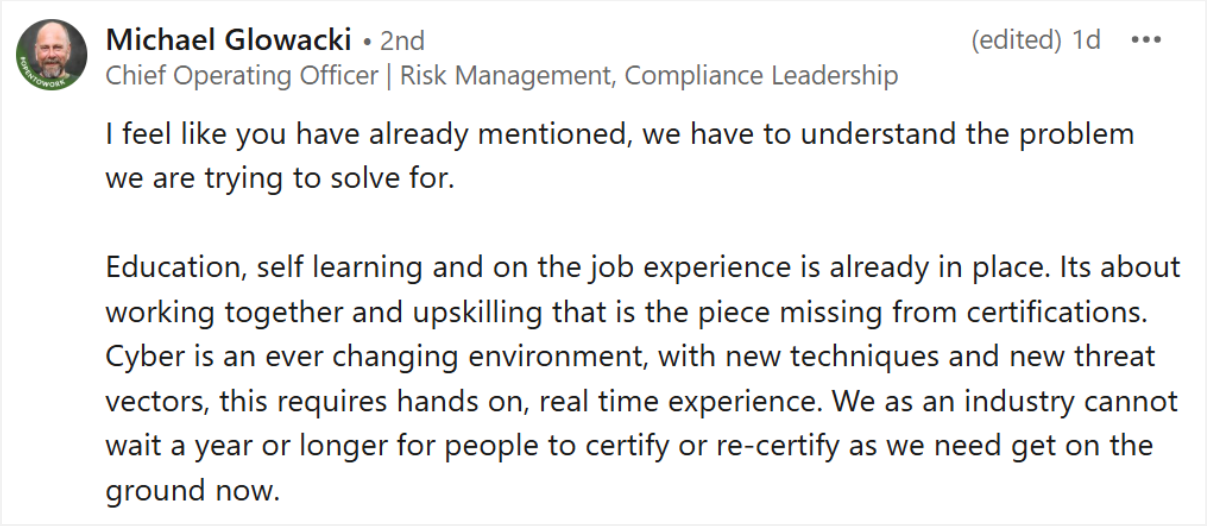
Michael Collins • 2nd 1h •••
Fractional CISO | Chief Systems Thinker | Coach | Independent Director

Thanks for sharing some of the history on this Nick Ellsmore it's helpful context for me. I'm sceptical (vs cynical) about the value of the scheme and would echo the questions about whether we have the problem statement nailed down sufficiently.
Every new framework, standard and scheme we introduce increases the complexity of our industry and creates further confusion for our customers. I have not seen enough evidence yet to support the proposal at this time. If that evidence is forthcoming I'll reconsider as any good sceptic should.

Source

Michael Glowacki, COO at Sphere (20 years of experience)

On the 21st of January 2025, Michael published this:



Michael Glowacki • 2nd (edited) 1d •••
Chief Operating Officer | Risk Management, Compliance Leadership

I feel like you have already mentioned, we have to understand the problem we are trying to solve for.

Education, self learning and on the job experience is already in place. Its about working together and upskilling that is the piece missing from certifications. Cyber is an ever changing environment, with new techniques and new threat vectors, this requires hands on, real time experience. We as an industry cannot wait a year or longer for people to certify or re-certify as we need get on the ground now.

[Source](#)

Michael Loss, Red Team Manager at CrowdStrike (15 years of experience)

On the 22nd of January 2025, Michael published this:

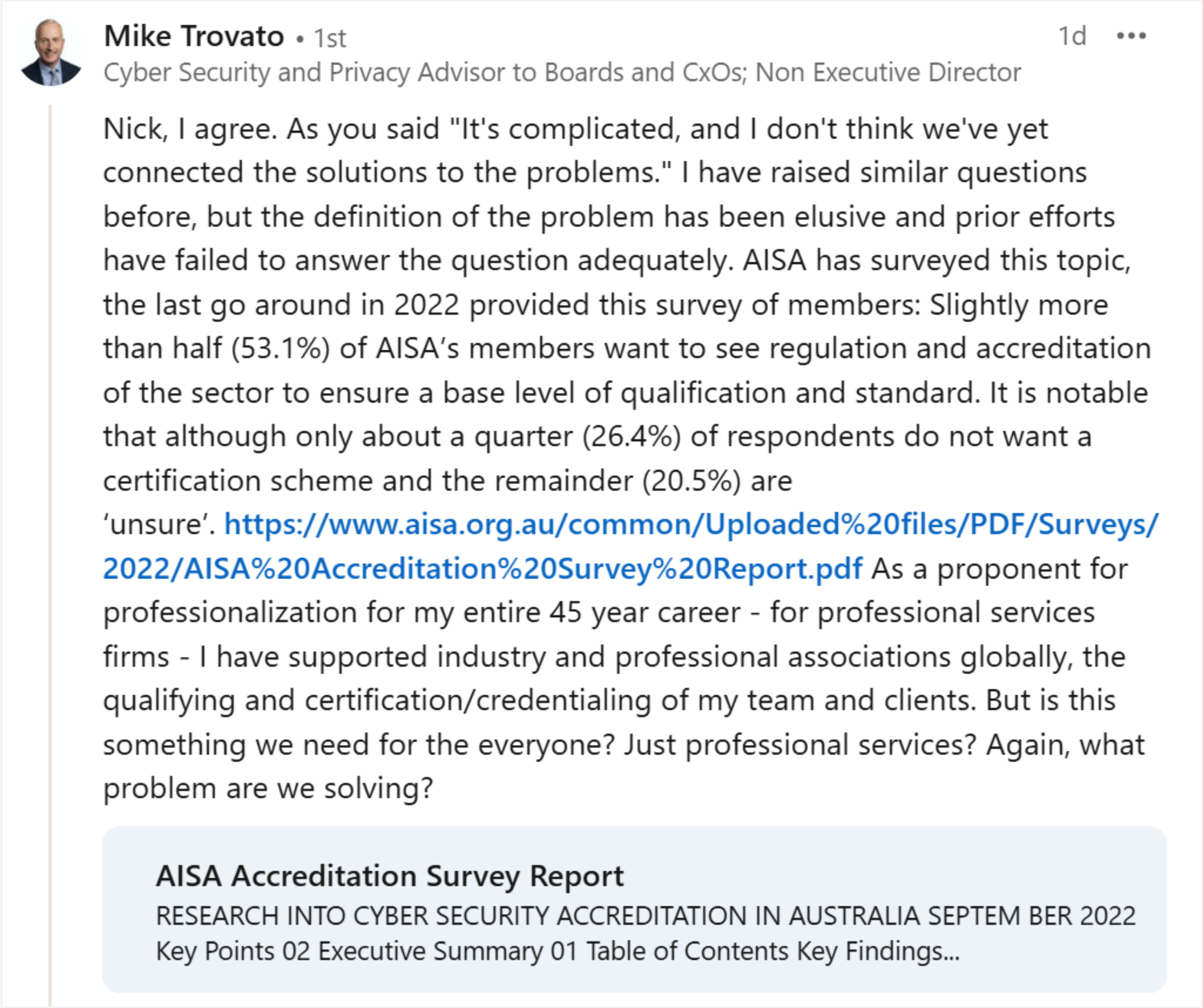
> Benjamin Mossé has done a great job here outlining many of the issues with "professionalisation" of the cybersecurity sector. Recommended reading, as is this one from Nick Ellsmore: https://lnkd.in/gbjiJyGX
>
> A few extra points from me:
>
> Yes, we have a problem. Huge portions of the cybersecurity industry are essentially a 'market for lemons' in which it's close to impossible for many customers to meaningfully assess the quality of products and services that they're procuring. This has led to a glut of low-cost, low-effort, cash-grab operations, selling products that barely function and/or services that provide close to zero value.
>
> I've seen the garbage flooding the market continue to drag down customer expectations, along with willingness to invest in those products and services that actually provide value. It is maddening how many times in my career I have heard customers express pleasant surprise at their first time receiving a pentest or red team report that wasn't just regurgitated "scanner trash".
>
> Unfortunately, advocates for professionalisation schemes like this are very clearly falling for the politician's fallacy, i.e. "We must do something. Professionalisation is something. Therefore, we must do professionalisation.".
>
> Any such scheme will inevitably fall into just another form of regulatory capture, in which the big players will game the system to block otherwise-capable yet less-well-resourced entrants to the sector, while also doing the bare minimum to ensure that their own staff with dismal skills and near-zero experience are still "technically compliant". The end result: "shiny garbage".
>
> Anyone who knows me well has probably heard me rant about Goodhart's Law (https://lnkd.in/gxZZKemi),

> often summarised as "When a measure becomes a target, it ceases to be a good measure". If you create a set of rigidly-defined hoops that must be jumped through to achieve entry into the field, don't be surprised when you get practitioners that are heavily optimised for the hoops, and mostly useless in the field.

Source: https://www.linkedin.com/posts/michael-loss-8a101074_professionalization-scheme-proposal-activity-7287705657816891392-LTu_/

Mike Trovato, Managing Partner at Cyber Risks Advisors, ex EY and KPMG Partner (45 years of experience)

On the 21st of January 2025, Mike published this:



Mike Trovato • 1st 1d •••

Cyber Security and Privacy Advisor to Boards and CxOs; Non Executive Director

Nick, I agree. As you said "It's complicated, and I don't think we've yet connected the solutions to the problems." I have raised similar questions before, but the definition of the problem has been elusive and prior efforts have failed to answer the question adequately. AISA has surveyed this topic, the last go around in 2022 provided this survey of members: Slightly more than half (53.1%) of AISA's members want to see regulation and accreditation of the sector to ensure a base level of qualification and standard. It is notable that although only about a quarter (26.4%) of respondents do not want a certification scheme and the remainder (20.5%) are 'unsure'. https://www.aisa.org.au/common/Uploaded%20files/PDF/Surveys/2022/AISA%20Accreditation%20Survey%20Report.pdf As a proponent for professionalization for my entire 45 year career - for professional services firms - I have supported industry and professional associations globally, the qualifying and certification/credentialing of my team and clients. But is this something we need for the everyone? Just professional services? Again, what problem are we solving?

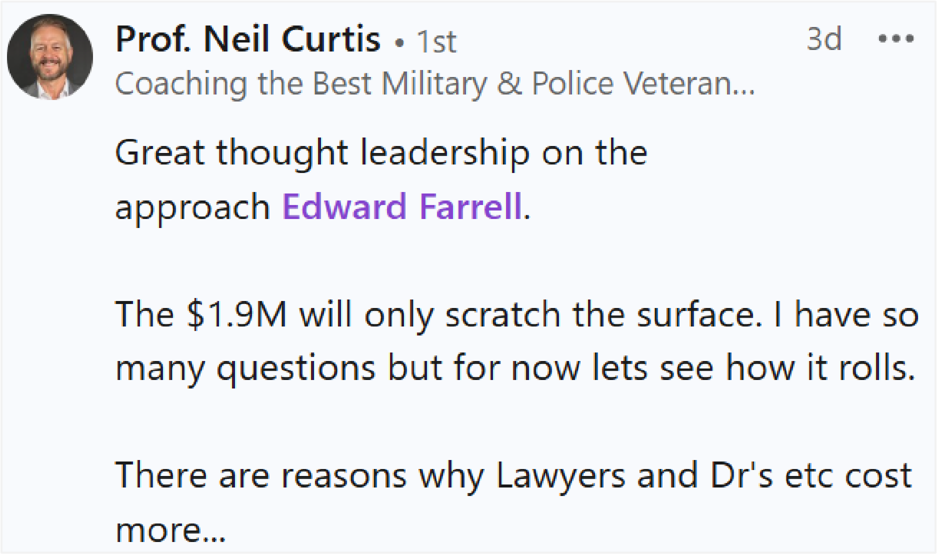
AISA Accreditation Survey Report

RESEARCH INTO CYBER SECURITY ACCREDITATION IN AUSTRALIA SEPTEM BER 2022 Key Points 02 Executive Summary 01 Table of Contents Key Findings...

Source

Neil Curtis, Professor, Executive Innovator at Solve Transition (20 years of experience)

On the 20th of January 2025, Neil published this:



Prof. Neil Curtis • 1st 3d •••

Coaching the Best Military & Police Veteran...

Great thought leadership on the approach Edward Farrell.

The $1.9M will only scratch the surface. I have so many questions but for now lets see how it rolls.

There are reasons why Lawyers and Dr's etc cost more...

Source

Nick Ellsmore, Cyber security business builder (25 years of experience)

On January 21st 2025, Nick published this:

Those who have been in the industry for a long time (20+ years) would remember that we've been down this path multiple times before. 20 years ago, I led a project for the Dept of Communications, IT & the Arts, looking at exactly this: it was called "IT Security Skills Certification in Australia". (Some of the reporting on it at the time is still online, eg https://www.zdnet.com/article/no-need-for-aussie-it-security-certification/)

...and for absolute clarity, the fact that I looked at the problem 20 years ago and concluded one thing, does not mean that it's still the right answer. The market is wildly different now, to what it was then. I understand that. But the heart of the problem we're trying to solve - and why it's hard to solve - I don't think has changed.

(Incidentally, I believe AISA has a copy of that report which was released under Freedom of Information... I don't have a copy myself or I'd re-share it).

In that project 20 years ago, we held dozens of industry meetings and had involvement from all the key stakeholders, and what we found was that there are 3 different things that a "professionalisation" scheme is generally trying to "validate" about a person, of differing levels of importance/value to different participants in the process:

1. Knowledge - do you know a certain baseline of stuff

2. Practical Expertise - can you apply that knowledge

3. Integrity - can we trust you with significant access

> Part of the challenge is that these 3 things are very different and routinely get conflated or misrepresented.
>
> We already have plenty of options for #1. In fact part of what dropped out of the "IT Security Skills Certification in Australia" work was an identification that some aggregated information was needed, and APEC stepped in to fund this: https://www.apec.org/docs/default-source/Publications/2007/5/APEC-Guide-to-Information-Security-Skills-Certification-Booklet-May-2007/07_tel_skills_guide.pdf. In 2017, Hivint put together an updated version of that, referenced here: https://medium.com/hivint-blog/introducing-the-cyber-security-skills-career-guide-f38261f39adc
>
> The issue that those guides tried to address is that people still mis-use the existing programs. Asking for a CISSP for a penetration tester is pointless. Realistically though, they obviously didn't have the reach or cut-through that would have made a difference. (Plus they were our subjective view, and your view of the utility of Cert A for Purpose B may be different to ours)
>
> The real challenges I think we are dealing with are:
>
> #2 in the list above - ie, not just whether someone knows a thing, but whether they can actually do something effectively with that knowledge... with the particular challenge being that the way I want something done is almost certainly different to the way someone else wants that same something done.
>
> #3 in the list above - This idea that agreeing to a "code of ethics" achieves #3 is farcical... That's why Govt doesn't make you agree to a code of ethics when you join the intelligence agencies, it makes you go through a very detailed clearance process, at a level appropriate to the sensitivity you'll be exposed to. In the private sector we don't have access to the clearance process. This is arguably the easiest problem to solve - it would cost money, and introduce obvious privacy concerns, but the mechanism is there.
>
> And then of course there's the history of failed attempts at this. AISA for a while had an "AISA Professional" membership level which was intended to be a professionalisation scheme. AusCERT likewise introduced their own, called ISSPCS. CREST has been trying to expand into this space (beyond penetration testing) for quite a few years. The Australian Computer Society (ACS) would I'm sure love to run such a scheme to give them relevance in 2025. AustCyber and its evolutions likewise. It is every industry non-profit's dream to have control of a mandatory licensing scheme.
>
> There can't be serious debate about whether or not a professionalisation scheme creates a barrier to entry. Of course it does - that's the whole point! The only question is whether that barrier makes things better, through keeping charlatans out, or makes things worse, through suppressing supply of cybersecurity services. I don't have an answer to that.

Source: https://www.linkedin.com/pulse/cyber-security-skills-certification-australia-here-we-nick-ellsmore-jlyhc/

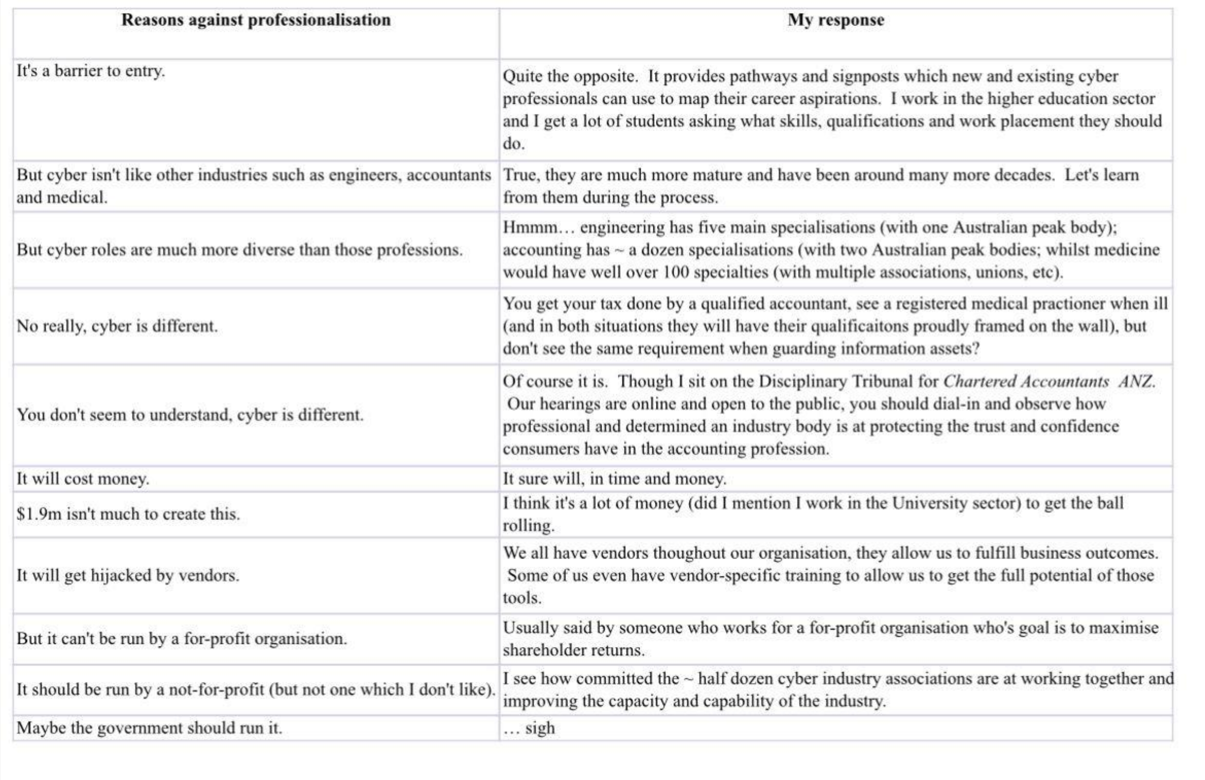
Nigel Phair, Professor at Monash University and Chair at CREST (20 years of experience)

On the 20th of January 2025, Nigel published this:

> Professional cybers ... I've been reading many of the posts espousing the positive and

negative aspects of a professionalisation scheme.

So here is my 2 cents.

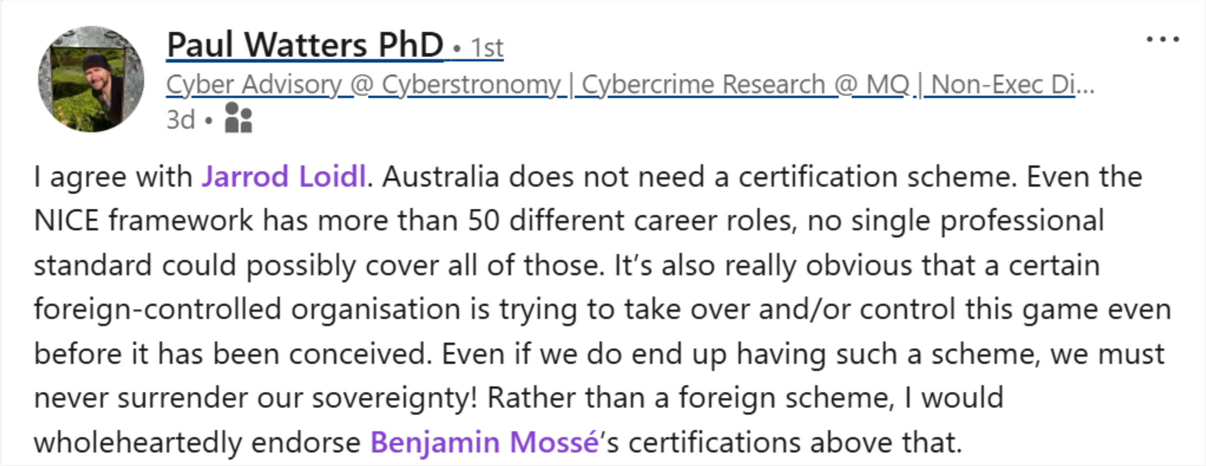


Reasons against professionalisation	My response
It's a barrier to entry.	Quite the opposite. It provides pathways and signposts which new and existing cyber professionals can use to map their career aspirations. I work in the higher education sector and I get a lot of students asking what skills, qualifications and work placement they should do.
But cyber isn't like other industries such as engineers, accountants and medical.	True, they are much more mature and have been around many more decades. Let's learn from them during the process.
But cyber roles are much more diverse than those professions.	Hmmm… engineering has five main specialisations (with one Australian peak body); accounting has ~ a dozen specialisations (with two Australian peak bodies; whilst medicine would have well over 100 specialties (with multiple associations, unions, etc).
No really, cyber is different.	You get your tax done by a qualified accountant, see a registered medical practioner when ill (and in both situations they will have their qualificaitons proudly framed on the wall), but don't see the same requirement when guarding information assets?
You don't seem to understand, cyber is different.	Of course it is. Though I sit on the Disciplinary Tribunal for *Chartered Accountants ANZ*. Our hearings are online and open to the public, you should dial-in and observe how professional and determined an industry body is at protecting the trust and confidence consumers have in the accounting profession.
It will cost money.	It sure will, in time and money.
$1.9m isn't much to create this.	I think it's a lot of money (did I mention I work in the University sector) to get the ball rolling.
It will get hijacked by vendors.	We all have vendors thoughout our organisation, they allow us to fulfill business outcomes. Some of us even have vendor-specific training to allow us to get the full potential of those tools.
But it can't be run by a for-profit organisation.	Usually said by someone who works for a for-profit organisation who's goal is to maximise shareholder returns.
It should be run by a not-for-profit (but not one which I don't like).	I see how committed the ~ half dozen cyber industry associations are at working together and improving the capacity and capability of the industry.
Maybe the government should run it.	… sigh

Source

Paul Watters, vCISO, Honorary Professor (20 years of experience)

On the 20th of January 2025, Paul published this:



Paul Watters PhD • 1st

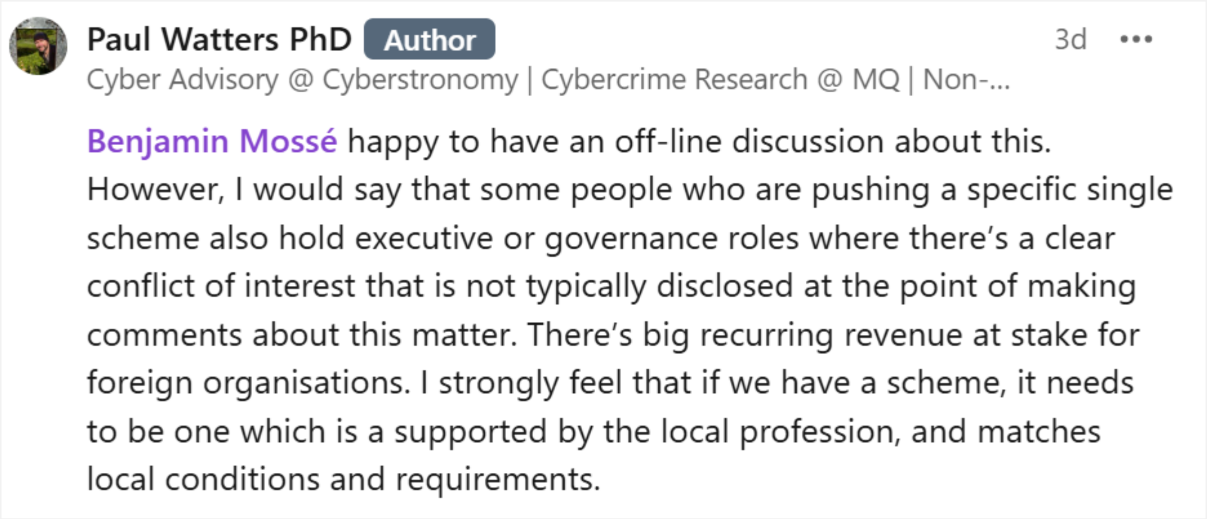
Cyber Advisory @ Cyberstronomy | Cybercrime Research @ MQ | Non-Exec Di...

3d •

I agree with Jarrod Loidl. Australia does not need a certification scheme. Even the NICE framework has more than 50 different career roles, no single professional standard could possibly cover all of those. It's also really obvious that a certain foreign-controlled organisation is trying to take over and/or control this game even before it has been conceived. Even if we do end up having such a scheme, we must never surrender our sovereignty! Rather than a foreign scheme, I would wholeheartedly endorse Benjamin Mossé's certifications above that.

Source

He also said this:



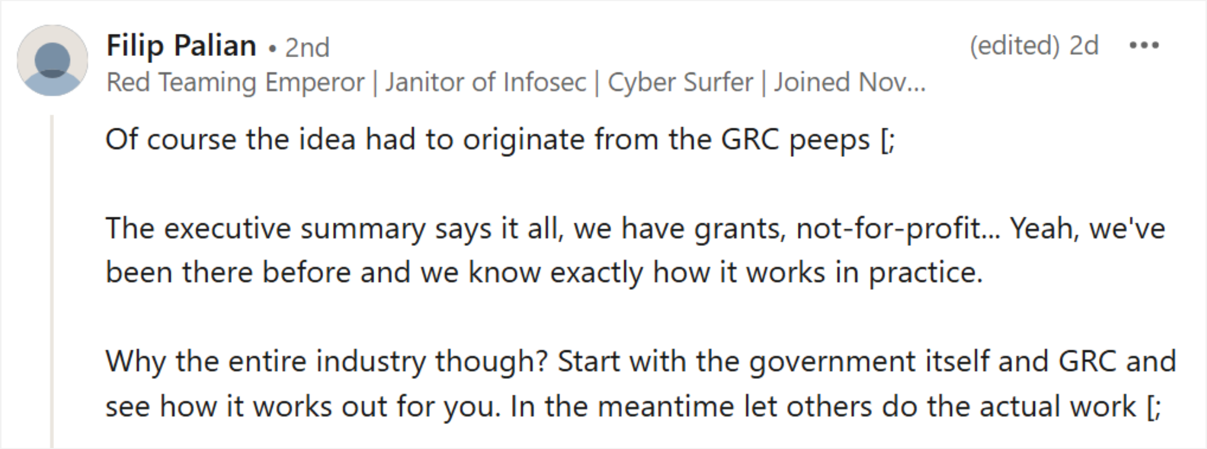
Paul Watters PhD Author 3d •••
Cyber Advisory @ Cyberstronomy | Cybercrime Research @ MQ | Non-...

Benjamin Mossé happy to have an off-line discussion about this. However, I would say that some people who are pushing a specific single scheme also hold executive or governance roles where there’s a clear conflict of interest that is not typically disclosed at the point of making comments about this matter. There’s big recurring revenue at stake for foreign organisations. I strongly feel that if we have a scheme, it needs to be one which is a supported by the local profession, and matches local conditions and requirements.

Source

Filip Palian, Red Teamer Emperor at CONFIDENTIAL (20 years of experience)

On the 20th of January 2025, Filip published this:



Filip Palian • 2nd (edited) 2d •••
Red Teaming Emperor | Janitor of Infosec | Cyber Surfer | Joined Nov...

Of course the idea had to originate from the GRC peeps [;

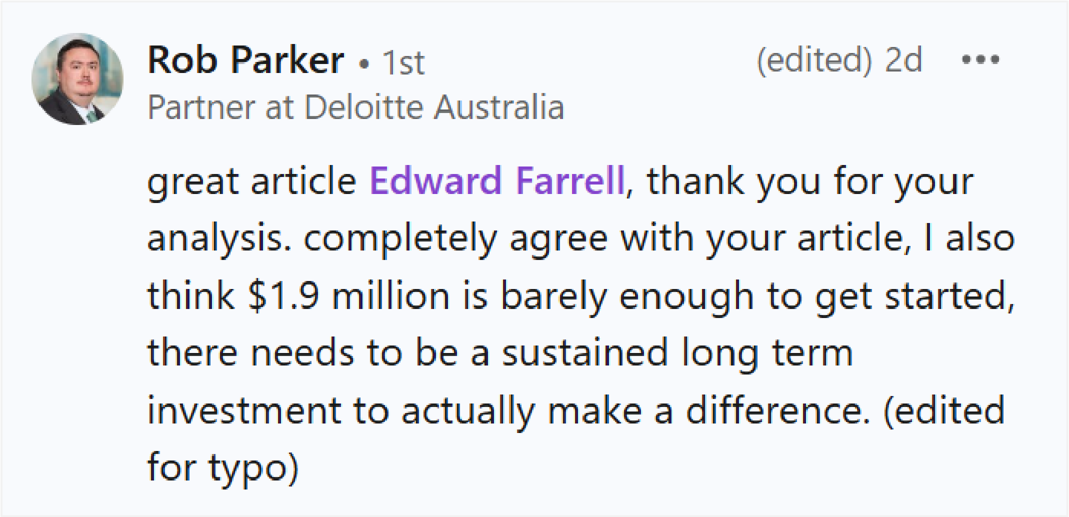
The executive summary says it all, we have grants, not-for-profit... Yeah, we've been there before and we know exactly how it works in practice.

Why the entire industry though? Start with the government itself and GRC and see how it works out for you. In the meantime let others do the actual work [;

Source

Rob Parker, Partner at Deloitte Australia (30 years of experience)

On the 21st of January 2025, Rob published this:



Rob Parker • 1st (edited) 2d •••

Partner at Deloitte Australia

great article Edward Farrell, thank you for your analysis. completely agree with your article, I also think $1.9 million is barely enough to get started, there needs to be a sustained long term investment to actually make a difference. (edited for typo)

Source

Shane Moffitt, ex Deputy CISO of the Victorian Government (20 years of experience)

On the 23rd of January 2025, Shane published this:

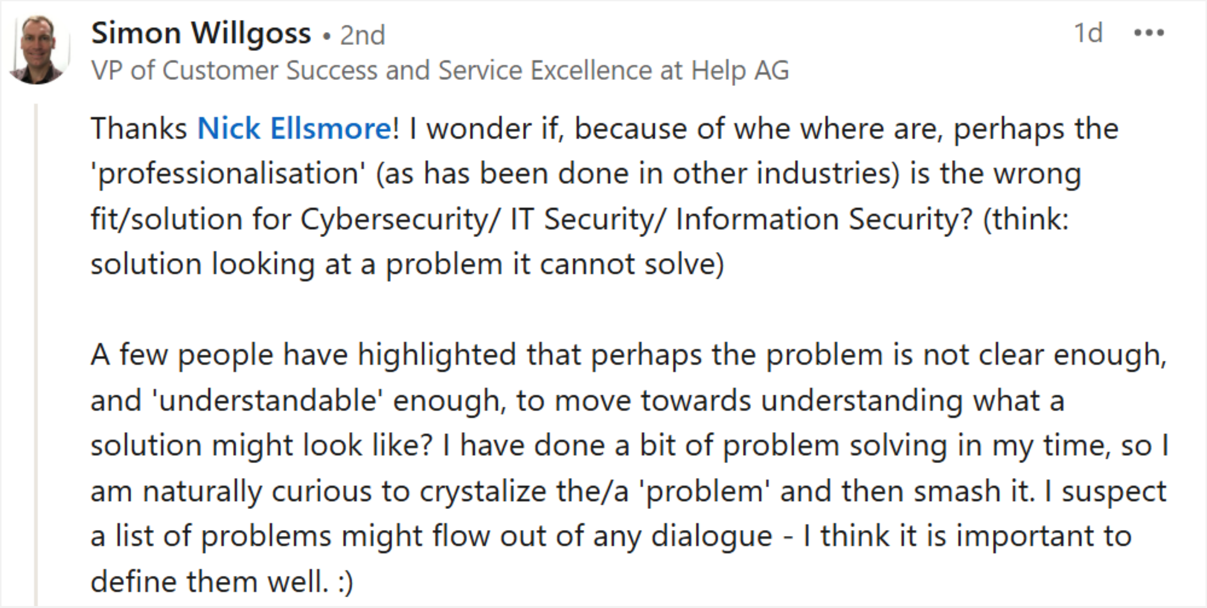
> Why I think the "Professionalisation Scheme for Australia's cyber security workforce" is a bad idea.
>
> In short, this is similar to a Certified Practising Accountant (CPA) or Bar Exam (becoming a Barrister) type program, but it is for Cyber professionals instead.
>
> The federal government has released a grant for this program, so no doubt intends on progressing this.
>
> https://lnkd.in/gHsruTKH
>
> While I applaud investing in improving a skilled Australian cyber workforce, I don't think this program will work.
>
> Having been responsible for looking at large-scale cyber workforces, including Whole of the Victorian Government with 350,000+ total staff (reiterating this is my opinion, not Vic Gov policy). I am firmly of the opinion that there are many different skillsets that consist of being a Cyber Professional.
>
> This can consist of human psychology, change management, deep technology knowledge of a particular technology, standards compliance, architecting multi-domain solutions, research, project management, incident response communications, incident response digital forensics, strategy, physical security, contract law, cryptography, software development, software testing ect, ect.
>
> In my 20+ years in the industry, I have never met a person who is competent across all of these domains.
>
> So, I only see two options for this framework.
>
> One - Some group makes an arbitrary decision about what skills a Cyber Professional should have, and those who don't have it are not deemed worthy.

> Two - It is so vague that anyone can get it, it adds no value but presents as a barrier/cost to entry for people trying to get into the field.
>
> Why does this work for other industries but not cyber? Basically, you can put the required skillsets into a cleaner, smaller box. "Cyber" is way too broad.

Source: https://www.linkedin.com/feed/update/urn:li:activity:7288052200990248960/

Simon Willgoss, VP of Customer Success at Help AG (25 years of experience)

On the 21st of January 2025, Simon published this:



Simon Willgoss • 2nd 1d •••
VP of Customer Success and Service Excellence at Help AG

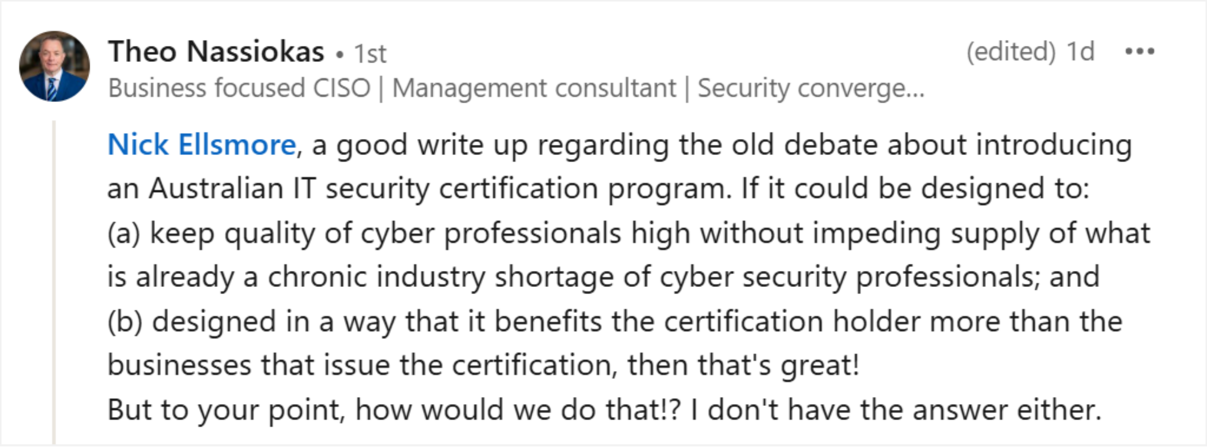
Thanks Nick Ellsmore! I wonder if, because of whe where are, perhaps the 'professionalisation' (as has been done in other industries) is the wrong fit/solution for Cybersecurity/ IT Security/ Information Security? (think: solution looking at a problem it cannot solve)

A few people have highlighted that perhaps the problem is not clear enough, and 'understandable' enough, to move towards understanding what a solution might look like? I have done a bit of problem solving in my time, so I am naturally curious to crystalize the/a 'problem' and then smash it. I suspect a list of problems might flow out of any dialogue - I think it is important to define them well. :)

Source

Theo Nassiokas, Co-Founder and President at Cyber8Lab (30 years of experience)

On the 21st of January 2025, Theo published this:



Theo Nassiokas • 1st (edited) 1d •••

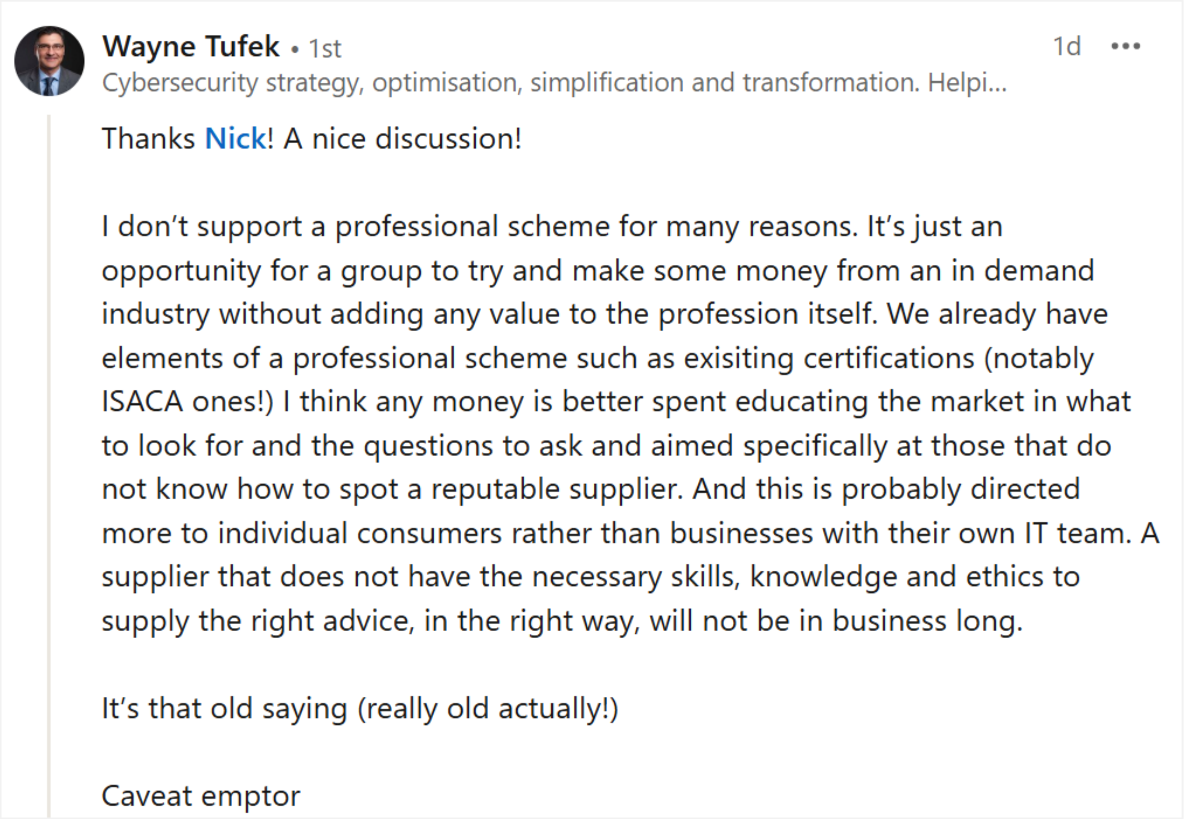
Business focused CISO | Management consultant | Security converge...

Nick Ellsmore, a good write up regarding the old debate about introducing an Australian IT security certification program. If it could be designed to:
(a) keep quality of cyber professionals high without impeding supply of what is already a chronic industry shortage of cyber security professionals; and
(b) designed in a way that it benefits the certification holder more than the businesses that issue the certification, then that's great!
But to your point, how would we do that!? I don't have the answer either.

Source

Wayne Tufek, Director at CyberRisk (20 years of experience)

On the 21st of January 2025, Wayne published this:



Wayne Tufek • 1st 1d •••

Cybersecurity strategy, optimisation, simplification and transformation. Helpi...

Thanks Nick! A nice discussion!

I don't support a professional scheme for many reasons. It's just an opportunity for a group to try and make some money from an in demand industry without adding any value to the profession itself. We already have elements of a professional scheme such as exisiting certifications (notably ISACA ones!) I think any money is better spent educating the market in what to look for and the questions to ask and aimed specifically at those that do not know how to spot a reputable supplier. And this is probably directed more to individual consumers rather than businesses with their own IT team. A supplier that does not have the necessary skills, knowledge and ethics to supply the right advice, in the right way, will not be in business long.

It's that old saying (really old actually!)

Caveat emptor

Source