Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A Model for Licensing IT Security

Is it feasible to license IT security professionals? By comparing the IT security profession to other licensed professions--medical doctors, civil engineers, CPAs and master electricians--this paper explores the difficulties involved in setting up licensing for IT security professionals as proposed in a 2009 U.S. Senate bill. After applying lessons from other professions, this paper argues that most of the difficulties can be resolved as long as the scope of practice for a licensed IT security professional is limited t...

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
Counter Tack Active Monitoring for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

A Model for Licensing IT Security

GIAC (GLEG) Gold Certification

Author: Mason Pokladnik, mason@schwanda.cc
Advisor: Benjamin Wright

Accepted: June 10th 2013

Abstract

Is it feasible to license IT security professionals? By comparing the IT security profession to other licensed professions—medical doctors, civil engineers, CPAs and master electricians—this paper explores the difficulties involved in setting up licensing for IT security professionals as proposed in a 2009 U.S. Senate bill. After applying lessons from other professions, this paper argues that most of the difficulties can be resolved as long as the scope of practice for a licensed IT security professional is limited to areas where it is most needed, such as critical infrastructure.

© 2013 SANS Institute, Author retains full rights.

© 2013 The SANS Institute Author retains full rights.

1. Introduction

In 2009, the United States' Senate considered legislation that would require the Department of Commerce to create a national licensing, certification and recertification program for information security professionals (Rockefeller, 2009). As the 2009 and later bills failed, movement at the Federal level has been limited to the form of Executive Orders, such as PPD/21 from Feb 12th, 2013, and internal efforts in the Department of Homeland Security (DHS) and the Department of Defense (DoD) with its Directive 8570 requirements (Committee, 2012). These efforts attempt to answer questions all organizations face in their security programs: How do I know the people in charge of IT security—or an outside consultant—know what they are doing? How do I know that the people in charge of developing software have the knowledge and incentive to follow secure development processes?

These same questions were also raised in the book *Geekonomics* and the CSIS report "A Human Capital Crisis in Cybersecurity." While no one sees licensing as a cure-all for the situation, people who have a license—and livelihood—to lose have an incentive to ensure that projects are carried out with a certain standard of care.

Since most IT jobs in the United States have no form of professional licensing—and the myriad of certifications available have clouded the picture so much that it is difficult to say what value any one may bring to a particular job title—this paper will evaluate some of the issues a licensing system for IT security professionals would need to address.

Implementers of a licensing system face difficulties:

- The lack of an industry-wide common body of knowledge
- What should be tested for an entry level professional, and what should be tested for an experienced professional to ensure competence yet not create a barrier to entry for talented young practitioners?
- An accreditation infrastructure for educational institutions
- The rapid pace of innovation in the industry

© 2013 The SANS Institute Author retains full rights.

- Almost all professional licensing is handled at the state level instead of the national level
- Defining when licensure is required

This paper will examine these difficulties, and evaluate what lessons we can apply to the licensing model by examining current licensing practices from other industries, such as the engineering, trade and medical professions. It will argue that by narrowing the scope of IT security licensing to the areas of critical infrastructure and services offered to the public, a system can be created that can improve the security of the nation without destroying the flexibility to innovate.

2. Difficulties Arising From Licensing IT Security

2.1. The Status Quo Does Not Prove Competence

In the Senate bill mentioned previously, one of many issues left to the Secretary of Commerce is to decide when it is appropriate to merely certify IT security skills and when to require a license of some type. There are already numerous existing IT security and audit certifications as well as a small group of secure software development certifications. As of April, 2013, there is even a software engineering licensing exam that can be used in Texas and Florida (Engineers, 2013). A major issue is, with the exception of the new Professional Engineering (PE) license, it is difficult to determine which certifications actually validate competency.

The DoD attempted to address this through the Directive 8570 program, but is still having difficulty identifying which certifications cost-effectively prove that people have the needed skills to secure networks. Now that the DoD is preparing to greatly expand its cyber command, the problems will be magnified. (Fryer-Biggs, 2013).

2.1.1. Common Body of Knowledge – A Work in Progress

An underlying issue is the lack of an industry-wide Common Body of Knowledge (CBK). $(ISC)^2$ made an early attempt at creating a CBK for security practitioners with the 10 domains covered by the CISSP, but the industry now needs to take the concept further. A single CBK for each focus area in IT security would define the knowledge and

© 2013 The SANS Institute Author retains full rights.

skills needed at different career stages; it would also eliminate the need to keep today's multiple CBKs current as practices change.

Software engineering is far ahead of the rest of IT security as its body of knowledge is organized under the IEEE computer society (n.d.). This gives software developers a strong organization leading the development of their CBK, whereas the general IT security practitioners are left with competing, for-profit vendors trying to out-market each other. Until the rest of IT security moves to a neutral industry-wide CBK, the current state of confusion will remain.

2.1.2. Existing Certifications Try to Serve Both Entry and Experienced Practitioners

Let's look at the overlapping knowledge domains from two 8570 approved certifications that require previous experience. They purport to certify that someone is capable of completing many job tasks under limited supervision (Defense, 2013):

CISSP ((ISC)^2, n.d.)	CASP (CompTIA, 2013)
• Access Control • Telecommunications and Network Security • Information Security Governance and Risk Management • Software Development Security • Cryptography • Security Architecture and Design • Operations Security • Business Continuity and Disaster Recovery Planning • Legal, Regulations, Investigations and	• Enterprise Security • Risk Management, Policy/Procedure and Legal • Research & Analysis • Integration of Computing, Communications, and Business Disciplines

© 2013 The SANS Institute Author retains full rights.

Compliance • Physical (Environmental) Security	

The vendors behind both of these certifications would love for them to become the gateway into the information security field. Many HR departments unjustifiably think the absence of a CISSP from a resume requires automatic disqualification of a candidate. Individuals have gone back and taken the CISSP for that reason alone.

However, these certifications are merely a test of fundamentals: Can you speak the language, apply test taking skills and understand basic concepts? This is incongruous with the experience requirements, as the day-to-day application of those basic concepts on a real network requires a deeper understanding.

Let's consider one fundamental concept from the risk management domain of both certifications. Both tests will expect candidates to understand that Risk = Threat X Vulnerability. Conceptually, this is true. If either of those components are zero, then there is no risk. Yet when both are non-zero, the components that make up Threat and Vulnerability in the real world are often subjective, difficult to measure and require an up-to-date inventory of the entire network that most organizations do not have. This is not just a simple multiplication problem.

An experienced professional knows that describing risk with a number is a very complex task. In the real world, politics, human psychology and other subjective factors do not lend themselves to discrete numbers. Even the best case for generating a vulnerability value—a localized CVSS score—has 14 inputs (N. I. f. S. a. Technology, n.d.). A typical audit and remediation tool would show that any sizable organization has thousands of identified applications across the network, assuming it tracks unique versions of each application. Additionally, an up to date set of threats is required, along with a way to prioritize the risks based on the value of the information or assets you are trying to protect.

It should be no surprise that an experienced professional's knowledge of risk management cannot be adequately assessed, together with all the other knowledge

© 2013 The SANS Institute Author retains full rights.

domains, during a 6 hour, 250 question test. One test cannot address the needs of both the entry level and experienced practitioner.

In the absence of a single CBK for the general IT security practitioner, opinions can vary widely as to what should be covered on a fundamentals of IT security exam. It would ideally take the best parts of several exams and combine them into something that addresses: vocabulary and concepts (something the CISSP does well); a strong audit focus both conceptually (techniques the CISA covers) and hands-on (like the GSNA); and application of theory to actual situations. A person passing the fundamentals exam should understand how to speak the language, create an auditable security control and know where to find the guidance necessary to turn the nebulous concept of risk into actual priorities to be worked on.

2.2. Why You Implicitly Trust Your Life to an Engineer

Engineering success usually means no one ever thinks about the job you did even though they implicitly trust their lives every day that it was done right. How does a profession earn such great public trust?

2.2.1. Engineers Integrate Lessons Learned in to their CBK for the Next Generation

Modern day engineering had to wait until the basic laws of nature could be described and predicted before they could be used to predict the performance of a structure. Today, using sophisticated finite element analysis programs, engineers can simulate how an explosion could affect a structure in order to understand how future designs might fail. In the case of September 11th, 2001, engineers spent years researching how the World Trade Center towers failed, with the goal of understanding how later designs might save more lives (N. I. o. S. a. Technology, 2005).

Engineering students are subjected to detailed analysis of disasters like the Space Shuttle Challenger explosion, partially to remind them of what is at stake. Students are then tested on the ethics of the decisions made leading up to the disasters. These lessons provide a balance to the pressures to reduce costs and speed the pace of construction.

© 2013 The SANS Institute Author retains full rights.

2.2.2. Trust is Built via Increasing Levels of Responsibility Over Time

The application of engineering concepts learned in school is supervised by an experienced, licensed professional. They provide guidance and real world experience, as a new graduate learns not just about how to design something, but also about the process of how it is actually built, on the way to earning a license to practice independently.

The path to obtaining a Professional Engineering (PE) license in civil engineering is well defined in the US. Once the educational requirements are met by graduating from an accredited program, one takes the Fundamentals of Engineering (FE) exam. Then, after working under a licensed engineer for approximately four years, an individual can take the PE exam. The PE exam is a more rigorous test that covers both knowledge of the entire field of civil engineering in the first half of the test, and your specific area of expertise in the second half (Surveying, 2012). Finally, the individual can apply in the local state to become a licensed Professional Engineer (Surveying, n.d.). Only after this progression of steps can an engineer actually approve documents for construction or issue engineering opinions as a service to the public—and then only within the areas of their expertise.

2.2.3. Licensed Professionals Limit Their Practice to the Areas of Their Expertise

A civil engineer could not responsibly approve electrical engineering plans or even other sub-specialties inside civil engineering if they were not competent to do so. Modeling a floodplain is an entirely different expertise from designing the structural elements for a skyscraper, yet both are licensed as civil engineering in some states.

2.2.4. Licensed Professionals Supervise Critical Life Safety Tasks

A licensed Professional Engineer (PE) must supervise and actually sign and seal their engineering opinions and drawings for services offered to the public. Not everyone working on a project has to be licensed, but the engineer of record does.

Most enterprises should not be required to have their internal security projects performed or overseen by a licensed professional. However, civil engineering teaches a lesson that should apply to certain IT security work. When public safety is at stake, a more qualified or licensed professional should supervise the process.

Mason Pokladnik, mason@schwanda.cc

© 2013 The SANS Institute, Author retains full rights.

© 2013 The SANS Institute Author retains full rights.

This paper argues the following two areas require this type of professional supervision: critical IT infrastructure and consulting services offered to the public.

2.2.5. General IT Security is Lacking in Accreditation and Examination Infrastructure

Software engineering has inherited an existing infrastructure of organizations that accredit professional engineering education and licensing including:

- ABET—which accredits a variety of technical degree programs including engineering, information systems and computer science degrees, but nothing specific to general IT security (ABET, n.d.).
- NCEES—which develops engineering licensing exams at the fundamental, professional and specialty levels on behalf of the state licensing boards.

There is no equivalent accreditation or testing infrastructure for general IT security practitioners. One non-profit organization was created at the recommendation of the CSIS report "A Human Capital Crisis in Cybersecurity" (Evans & Reeder, 2010). The National Board of Information Security Examiners (NBISE) was created in 2010 to "lead and coordinate a national response to the cyber security workforce crisis" (Examiners, n.d.). It would appear from their choice of name—and selection of the CSIS report's authors as leaders—that the NBISE believes it can develop examinations to validate IT professional's skills at various times in their career path. Unfortunately, exam development can be an expensive process, and it is unclear how they will generate the funding necessary for a self-sustaining organization.

The NBISE could serve as a neutral party for stewarding both the CBK and licensing exams. However, the NBISE has only conducted one trial test in the United States, and it is still in the early stages of defining what the various IT security roles and their associated competencies are.

2.3. Incompatibilities with the Engineering Model

The engineering model is not a perfect model for IT security. PE licensing takes place at the state level under varying sets of rules. Many states offer reciprocity to other states' license holders, but professionals must still register with each state individually

© 2013 The SANS Institute Author retains full rights.

and keep track of the separate laws within each state. This has led to some industries whose work spans multiple states, such as automotive engineers, to obtain exemptions from licensure ("Regulation and licensure in engineering," n.d.).

Since IT consulting and software development are portable professions, there would be a considerable issue if people were required to be licensed in every state in which they work.

States have a wide variety of laws regarding various IT disciplines. For digital forensics, Michigan requires a certification like the CISSP, while Texas requires a private investigators license (Moulton, 2008).

For the licensing of IT security, it appears that a consistent and more efficient policy is needed. Is that policy to exempt some disciplines from the need for licensing, to consolidate it at the federal level or to harmonize the various state laws? Another approach—instead of exempting a specific type of security practice—is to reduce the scope of activities where a license is required.

2.3.1. The HD Moore Problem – Experience Counts more than a Four Year Degree

It is not within the scope of this paper to offer a full CBK for IT security as many bright people are working on the issue, and one can see the CSIS report's summary of current activities starting on page 6 of the report.

However, this paper argues that the validation of hands-on skills should be at least as high of a priority as a traditional degree. A licensing or expert level certification exam should include an evaluation of real world experience.

The story of HD Moore helps illustrate this lesson. Every once in a while someone special like HD Moore comes along and makes the entire IT security industry take notice. The industry should want as many people of HD Moore's caliber to come work for the defensive security side as possible. The Metasploit framework project he founded is a weapon that can be used for auditing or attacking the infrastructure of a country—as many are fond of saying, the only difference is permission. Yet at age 17,

© 2013 The SANS Institute Author retains full rights.

HD was not running his own company offering his services to the government (Higgins, 2006). That is the role of an experienced professional.

The CBK for an expert IT security professional should include the concepts that cause tools, such as Metasploit, to be used responsibly. A licensed professional should understand the legal environment in which they operate, have enough project management skills to keep the doors open and people paid, enough knowledge of business to help their client (internal or external) prioritize IT related risks, and the experience of having learned from their own and other's mistakes over time. A licensed professional should possess the experience to be the interface between a 17 year old, like HD—who understands the fundamentals of software security at a deeper level than all but the absolute best and brightest in the world, but may not have a formal degree—and the US government.

What kind of licensing model keeps Metasploit a public project instead of being sold to the highest grey market bidder? If the lack of a 4 year degree from an accredited school were to have kept HD out of the legitimate security services market, then the model has a major flaw.

General IT security is not traditional engineering. Physics and Calculus are not prerequisites and neither are four year degrees. It would be imprudent to apply to general IT security the part of the professional engineering model that requires graduation from an accredited program before you can begin to practice.

2.4. A Lesson from the Medical Profession on the Rapid Pace of Innovation

IT has no exclusivity on the concept of rapid change. The medical profession has come a long way from, in the actual dark ages, being mostly a guessing game to today becoming a highly educated guessing game greatly informed by science. Medicine experiences rapid advances, but still manages to integrate new knowledge into its existing CBK taught to new medical school students.

After earning their M.D., newly graduated doctors do not take care of patients on their own. Instead, graduates become interns or residents, so they can gain experience

© 2013 The SANS Institute Author retains full rights.

actually working with patients. They eventually get their license to practice in a particular state after at least a year of hands on learning. After that, they may still need to finish their residency program and possibly a fellowship depending on what specialty area they choose to practice in before treating patients unsupervised.

2.4.1. Licensing is a Multi-Step Process over Different Career Stages

Similar to professional engineering, the medical licensure model is: accredited degree, testing of fundamentals—although in multiple steps (Examination, 2013), working under supervision and then ultimately a license allowing independent practice. Medicine offers a counter-example to those who argue that IT changes too rapidly to be able to test. Medical schools teach the knowledge that is current at the time, and doctors are responsible for continuing their education after they are licensed.

2.5. Trade Licensing – Apprentice, Journeyman, Master

There is one more licensing scheme to consider since it offers some of the benefits of both the engineering and medical models with less burdensome educational requirements. Many trades operate on the apprentice model, such as plumbers and electricians. Both of these trades are licensed and regulated by the state, but the educational requirements to get started are significantly lower as the expectation is that the individual will be learning and gaining experience on the job. This allows less experienced people to work in the field, but under varying degrees of supervision depending on the combination of their real world experience and education.

A master electrician is the product of a continuous learning process—both on the job and in class—with two licensing exams to verify their increasing expertise to oversee projects and less experienced members of their profession.

The steps to becoming a master electrician are (Bureau of Labor Statistics, 2012):

- A high-school diploma
- Either a 2 year associate's degree in electronics covering electrical theory, algebra and building codes or an extended apprenticeship program that offers these classes.

© 2013 The SANS Institute Author retains full rights.

- 2 year apprenticeship (4 without an associate's degree)
- Licensing exam – varies by state as there is no national test for electrician's license
- Either a bachelor's degree in electrical engineering or 7 years of experience.
- Exam for master electrician's license

If an objective of the IT security industry is to get people involved early, then allowing them to start an apprenticeship program right out of high-school or after an associate's degree is a considerably lower hurdle than either the 4 or 8 years of education required to enter the engineering or medical professions respectively.

The trade licensing model is already reflected in the training requirements of DoD directive 8570. As the level of responsibility increases, so does the requirement for certifications demonstrating competency to handle that responsibility. IAMs/IATs are already split into three experience levels and under the upcoming National Initiative for Cybersecurity Education (NICE) and DoD directive 8140 (the expected replacement for 8570) this alignment with the apprentice, journeyman, master model is even more intentional (Keith, 2013).

3. A Model for Licensing IT Security

This paper envisions a model of IT security where software security licensing and general IT security licensing are two separate paths. Since software engineering has already developed a body of knowledge with IEEE and a licensing exam through NCEES, it seems logical for it to continue developing as an engineering discipline. However, this paper argues the rest of IT security should follow a hybrid of the tradesman and medical licensing models.

3.1. Software Engineering, a more Disciplined Form of Software Development

The new bay bridge between San Francisco and Oakland California may be opened later than the originally planned Labor Day 2013 date. The delay stems from the need for civil engineers to evaluate the effect of oxidation on various elements of the

© 2013 The SANS Institute Author retains full rights.

bridge including bolts and post-tensioning tendons (Piller, 2010). Some of these issues are the result of design choices; some of them are construction issues, such as not applying corrosion protection in a timely fashion. These issues are not likely to be fatal to the bridge. As it is in a known seismic zone, the bridge has a safety factor built into the design and even a plan for post construction strengthening of the bridge if needed. What these issues affect is how much it is going to cost to maintain the bridge during its lifetime.

Civil engineering is a more mature a branch of engineering than software engineering at present. The construction administration procedures that identified the issues in the bay bridge are a standard part of the construction process for a building. However, it is far from standard practice to have a security review of a program's source code or to test the program for security vulnerabilities during software development.

Software engineers, like their civil engineering peers, need to develop standards to protect public safety. For software engineering to progress to the point where developers predict and plan for failures, secure development processes must become mainstream. Each vendor will have to decide for itself—after it meets some standard of care yet to be defined—how much it wants to invest in building a more secure codebase from the beginning versus maintaining that code after the fact.

Most of the components are already in place for a software branch of engineering. The current software engineering Principles and Practices (PE) exam already has a secure development section (Surveying, 2013), and accredited computer science programs already exist. As the IEEE updates the CBK for software engineering—including security—the accreditation process can be used to ensure that degree programs are incorporating the updates.

The NCEES will need to follow-up the new software engineering PE exam with a Fundamentals of Engineering (FE) exam specifically for software engineering. This is due to the general use FE exam covering content from physics and other classed that are not necessarily part of a computer science degree. These exams could be used along with a grand-fathering process for existing experienced developers to produce the first crop of licensed software engineers.

Mason Pokladnik, mason@schwanda.cc

© 2013 The SANS Institute Author retains full rights.

3.1.1. Narrowing the scope of licensing to Critical Infrastructure Software

There are practical limitations to licensing in that we need to define what engineered software is and when its use is required. Not all software needs to be developed under the supervision of a licensed professional engineer, but as Rice (2008, p. 7) puts it "software, like cement before it, is becoming the foundation of civilization."

A video game and the control system for a nuclear reactor are on opposite ends of the spectrum regarding public safety. Standards will have to be set so that the control systems that watch over critical infrastructure must run engineered software. Governments and private organizations will have to use engineered software for areas where the law requires it, and they will desire to purchase it if it is seen to reduce risk versus alternate options. Even when not required by law, some software vendors will choose to create engineered software because it can be used to differentiate their products in the marketplace. This limited scope leaves the majority of software unencumbered with the need for licensed professional supervision unless the market is willing to pay for it.

3.1.2. Altering the License Agreement – Engineered Software Should not be able to Limit Liability

An important concept in engineering is "practicing in the public interest." Engineered software will have to be held to a higher standard than other software, and the only way to enforce that standard is to apply liability to organizations that sell engineered software.

This is a complex issue since modern software is literally impossible to test completely. All of the possible inputs to an even moderately complex program could take years to test—if it could even be done at all. Then, in a "Reflections on Trusting Trust" moment, it is further impossible to verify that all of the tools that are used to build the software are not subtly altering it by optimizing the code for runtime.

Thankfully, perfection is not the goal. Engineers are held to the standard of what a reasonable peer would have done at the time the work was done. Many of the practices necessary to prevent catastrophic failure are already a part of the Software Engineering

© 2013 The SANS Institute Author retains full rights.

Body of Knowledge, and its development over time, along with the courts, will determine what "reasonable" is.

3.2. Licensing General IT security

This paper argues that applied IT security professionals should fall under a model resembling parts of trade licensing and parts of medical licensing. The initial licensing process should follow the tradesman model where anyone with a high school diploma can enter into an apprenticeship position, if that position provides entry level training appropriate to moving towards a licensed position. Smaller organizations can require an associate's degree from an accredited program while the military or other larger organizations can provide this training internally if desired. Apprentices should be denied administrative privileges until they pass a fundamental level certification.

After a minimum amount of time—at least a year for those with an associate's degree and two for those without— apprentices should be allowed to take a journeyman level licensing exam. The minimum experience requirement is needed because there are many things that do not arise in a classroom setting. Some are unique to a particular organization and others are more universal. But an apprentice level practitioner should observe how the people supervising them make decisions for a while to learn how IT security concepts are actually applied and prioritized. Journeyman level practitioners can begin to be given a level of autonomy. They should be able to handle routine tasks on their own and complete projects under varying levels of supervision. Ideally, they will mentor apprentice level duties while gaining further experience of their own in the field.

After at least 2 to 3 years of total experience, a journeyman level practitioner should be allowed to take the masters level licensing exam. This exam would encompass all of the elements of the CBK that are required for managing a security program including topics on supervision of personnel, budgeting, project management and a hands-on portion for demonstrating applied security concepts. Normally a master's level licensee should have an accredited bachelor's degree. However, candidates with extended experience should be able to apply for an exception to the degree requirement.

Mason Pokladnik, mason@schwanda.cc

© 2013 The SANS Institute Author retains full rights.

A master level license should be required to independently supervise critical IT systems "in the public interest." A licensee need not perform all of the work on a project, but they do need to supervise that the work was done properly. They should additionally verify that any controls implemented are appropriate and auditable, preferably in an automated fashion. In the case of an audit, they should determine that the results are correct, prioritized and qualified where insufficient evidence exists to verify a false positive result.

Both the journeyman and masters levels licensees should have a continuing education requirement to renew the license.

3.2.1. Narrowing the Scope of Licensing to Services Offered to the Public and Operating Critical Infrastructure

Not all organizations need licensed IT staff. Small businesses without IT staff cannot be expected to pay for licensed staff under the same rationale that they do not keep a licensed electrician on staff. A licensed consultant should be required when they acquire IT security services from a third party.

Licensed IT security professionals should include anyone designing and implementing security programs for the federal government, publicly traded corporations, organizations designated as owning critical infrastructure and anyone offering IT security services to the public as a consulting engagement. Specific exclusions may be needed for computer repair and data recovery services which do not require any analysis of the results. Specific implementation details should be left up to the SEC for publicly traded companies, DHS for critical infrastructure, etc.

3.3. State or National Licensing

An organization like NCEES or NBISE would be needed to develop nation-wide licensing exams, as well as to guide continuing development of the general IT security CBK.

Licensing could be handled at the state level through a model law. Most states should offer reciprocity to licensed individuals similar to engineering disciplines. However, state licensing and reciprocity raise a problem for multi-state and international

© 2013 The SANS Institute Author retains full rights.

organizations as IT systems are not in a clearly defined location like a construction project. This is precisely the reason that automotive and aerospace engineers are not licensed. One option is the IT security industry could be licensed at the national level as proposed in the original 2009 Senate bill. The other option is to harmonize state laws similar to another profession, the CPA.

Certified Public Accountants have the same issue with multi-state organizations. They are licensed at the state level and need to be licensed either in their home state, or the state in which the companies' headquarters that they are auditing is located. The precise location from which an attestation is issued determines which state's rules will be applied for the engagement. Since CPAs operate under Generally Accepted Accounting Principles (GAAP)—which are standardized nationwide—the American Institute of CPAs created the Uniform Accountancy Act. It allows CPAs to operate in multiple jurisdictions with a single license by creating substantially equivalent licensing standards in the states that have adopted it (CPAs, n.d.). This allows a CPA from Texas to audit a California company as long as: California is not the CPA's principle place of business, the CPA notifies the California Board of Accountancy and pays a notification fee (Accountancy, n.d.).

In drafting model law for states, a similar mobility provision can be included from the beginning to simplify things for both software engineers and general IT security professionals. People working for one organization should be able to register only in the state in which they live, and those offering services to the public across state lines should be allowed to register as individuals and companies under privileges afforded by a mobility provision.

3.4. Verifying Specialist Skills

In addition to a general IT security license, there are multiple areas of IT security specialization that could benefit from an additional certification from a national board similar to the ones in medicine. Doctors who wish to specialize in emergency medicine complete a fellowship after their residency and take an additional exam over and above their regular license to practice medicine (Specialties, n.d.). These national boards award a diploma good for several years that can be renewed if the maintenance requirements are

© 2013 The SANS Institute Author retains full rights.

met. For emergency medicine, this includes not just continuing education, but retesting on current topics and a process to benchmark the doctor's current practices against those of peers (Medicine, n.d.).

In the United Kingdom, the Council of Registered, Ethical Security Testers (CREST) validates the processes and competence of security testers by examining both theory and hands-on knowledge. The hands-on portion of the exam requires finding common vulnerabilities in a test network and documenting them. This same type of testing could be used to validate a specialist's skills in penetration testing, incident response, digital forensics and other specialties.

4. Conclusion

Each of the licensed professions analyzed in this paper has a defined common body of knowledge for entry into their ranks, a method for integrating new knowledge over time, and a single organization overseeing each step to licensure. The lessons from these professions argues that licensing IT security is possible for both software engineering and general IT security practitioners, if the scope of that licensing is limited to those areas that most need it.

Limiting licensing to critical infrastructure (electrical generation and distribution, military and intelligence, telecommunications, finance, food and water supply, etc.) improves the quality of the new electronic foundations of our society. Requiring a license to provide security services to the public allows people to trust that a professional will be supervising the process—something they can expect when calling a doctor, lawyer or plumber, but not necessarily from a vulnerability assessment.

Additionally, a limited licensing model does not encumber the creative use of software until such time as someone wishes to use it for critical purposes. Only then will the decision have to be made whether it is worth the additional resources to provide engineered software.

By finishing the common body of knowledge, providing a model law and creating a multi-step licensing process, a professional licensure system can be established which is

© 2013 The SANS Institute Author retains full rights.

familiar enough for state governments to adopt, and much more expedient to implement than the natural progression other professions had to go through over the course of—in some cases—centuries.

5. References

(ISC)[2]. (n.d.). CISSP Domains. Retrieved May 14th, 2013, from https://www.isc2.org/cissp-domains/default.aspx

ABET. (n.d.). What Kinds of Programs Does ABET Accredit? Retrieved Feb 19th, 2013, from http://www.abet.org/types-of-programs-abet-accredits/

Accountancy, C. B. o. (n.d.). Practice Privilege Handbook. Retrieved May 26th, 2013, from http://www.dca.ca.gov/cba/publications/pphandbook.pdf

Bureau of Labor Statistics, U. S. D. o. L. (2012). Occupational Outlook Handbook 2012-2013 Edition. Retrieved May 24th, 2013, from http://www.bls.gov/ooh/construction-and-extraction/electricians.htm

Committee, H. S. A. (2012). Cyberskills Task Force Report. Retrieved Feb 19th, 2013, from https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf

CompTIA. (2013). CompTIA Advanced Security Practitioner Certification Exam Objectives Retrieved May 14th, 2013, from http://certification.comptia.org/Libraries/Exam_Objectives/CASP_objectives.sflb.ashx

CPAs, A. I. o. (n.d.). History of CPA Mobility. Retrieved May 26th, 2013, from http://www.aicpa.org/Advocacy/State/Pages/SubstantialEquivalencyandPracticeMobility.aspx

Defense, D. o. (2013). DoD Approved 8570 Baseline Certifications. Retrieved May 14th, 2013, from http://iase.disa.mil/eta/iawip/content_pages/iabaseline.html

Engineers, T. B. o. P. (2013). Software Engineering. Retrieved May 26th, 2013, from http://engineers.texas.gov/software.html

Evans, K., & Reeder, F. (2010). A Human Capital Crisis in Cybersecurity. Retrieved May 18th, 2013, from http://csis.org/publication/prepublication-a-human-capital-crisis-in-cybersecurity

Examination, U. S. M. L. (2013). Licensing Bulletin. Retrieved May 20th, 2013, from http://www.usmle.org/bulletin/overview/

Examiners, N. B. o. I. S. (n.d.). Frequently Asked Questions. Retrieved May 18th, 2013, from https://www.nbise.org/home/about-us/faq

Fryer-Biggs, Z. (2013). Experts say DoD cyber workers undertrained. Retrieved Feb 19th, 2013, from http://www.federaltimes.com/article/20130216/DEPARTMENTS01/302160001/Experts-say-DoD-cyber-workers-undertrained

Higgins, K. J. (2006). HD Moore Unplugged. Retrieved June 1st, 2013, from http://www.darkreading.com/hd-moore-unplugged/208804089

Mason Pokladnik, mason@schwanda.cc

© 2013 The SANS Institute Author retains full rights.

Keith, S. L. (2013). Cyberspace Workforce January 2013 Retrieved May 14th, 2013, from http://www.afcea.org/events/west/13/documents/CyberspaceWorkforceKeith_000.pdf

Medicine, A. B. o. E. (n.d.). Maintenance of Certification Overview. Retrieved May 26th, 2013, from https://www.abem.org/PUBLIC/portal/alias__Rainbow/lang__en-US/tabID__3422/DesktopDefault.aspx

Moulton, S. (2008). Michigan To Require Certifications For Computer Forensics Private Investigators License. Retrieved May 19th, 2013, from http://computer-forensics.sans.org/blog/2008/12/05/michigan-requires-cissp-for-private-investigators-license

Piller, C. (2010). Corrosion Plagues New Bay Bridge Span. *Sacramento Bee*. http://www.sacbee.com/2013/05/18/5431401/corrosion-plagues-new-bay-bridge.html

Regulation and licensure in engineering. (n.d.). *Wikipedia*. Retrieved May 26th, 2013, from http://en.wikipedia.org/wiki/Regulation_and_licensure_in_engineering

Rice, D. (2008). *Geekonomics : the real cost of insecure software*. Upper Saddle River, NJ: Addison-Wesley.

Rockefeller, J. (2009). *S.773 - Cybersecurity Act of 2009*. Retrieved Feb 19th, 2013, from http://www.opencongress.org/bill/111-s773/show

Society, I. C. (n.d.). Guide to the Software Engineering Body of Knowledge (SWEBOK) V3. Retrieved May 26th, 2013, from http://www.computer.org/portal/web/swebok/v3guide

Specialties, A. B. o. M. (n.d.). Board Certification: the Process. Retrieved May 26th, 2013, from http://www.abms.org/who_we_help/physicians/process.aspx

Surveying, N. C. o. E. f. E. a. (2012). Principles and Practice of Engineering CIVIL BREADTH and STRUCTURAL DEPTH Exam Specifications. Retrieved May 30th, 2013, from http://cdn1.ncees.co/wp-content/uploads/2012/11/Exam-specifications_PE-Civil_PE-Civ-Structural-Apr-2008_with-1304-design-standards.pdf

Surveying, N. C. o. E. f. E. a. (2013). NCEES Principles and Practice of Engineering Examination Software Engineering Exam Specifications. Retrieved May 26th, 2013, from http://engineers.texas.gov/downloads/ncees_PESoftware_2013.pdf

Surveying, N. C. o. E. f. E. a. (n.d.). Licensure. Retrieved Feb 19th, 2013, from http://www.ncees.org/licensure

Technology, N. I. f. S. a. (n.d.). Common Vulnerability Scoring System Version 2 Calculator. Retrieved May 15th, 2013, from http://nvd.nist.gov/cvss.cfm?calculator&version=2

Technology, N. I. o. S. a. (2005). Federal Building and Fire Safety Investigation of the World Trade Center Disaster. *Part IIB – Collapse Sequence.* Retrieved May 13th, 2013, from http://www.nist.gov/el/disasterstudies/wtc/upload/WTC_Part_IIB_CollapseSequence_Final.pdf

Mason Pokladnik, mason@schwanda.cc

© 2013 The SANS Institute Author retains full rights.

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced