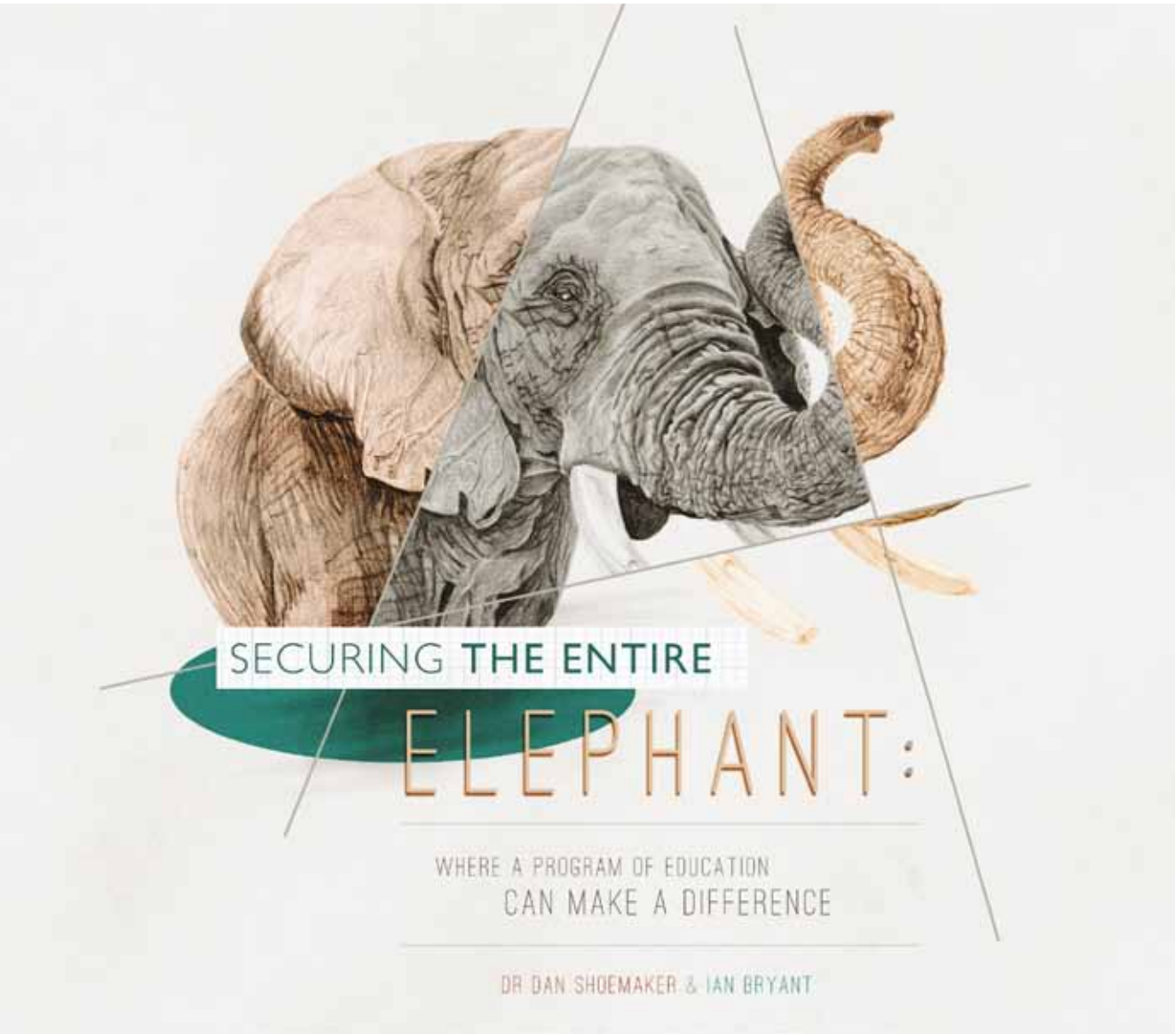

The global economy rests on a technology base. So, it is common sense to make certain that that technology is secure. Sadly, current data from almost any source indicates that our systems are not secure.

The principal cause seems to be what might be called the "Six Blind Men and the Elephant" syndrome. In that old story six blind men are asked to describe an elephant based on what they are touching. So to one it's a snake, to another a wall, and to another a tree, etcetera. In the end, "Though each was partly in the right, all were entirely wrong". We have the same problem with cybersecurity. There are established elements of the field that know how to secure the part of the technology that they touch. But until we are able to coordinate that knowledge to secure the whole elephant, we can't realistically say we are secure. Or in pragmatic terms, "partly" secure simply does not suffice. Probably the best illustration of that old adage is the U.S. National Security Agency, which was done in by an insider exploit, not the electronic one that they were set up to prevent. This is where formal education comes in. Education shapes behaviour. For that reason, education can be an extremely powerful force for ensuring correct practice. Also, it is education's historical impact on society at large that makes it the most likely place to address the need for comprehensive cybersecurity.

Nevertheless, there are a number of challenges that have to be overcome. First, according to a report from the National Academies of Science, cybersecurity is an emerging discipline. Consequently, it is not clear what should be taught. Worse, all evidence points to the fact that whatever we should be teaching is cross-cutting. In essence, elements of the discipline could be taught in places as diverse as engineering, business, and law. These are different academic cultures, and cybersecurity practice is viewed differently in each. This cultural difference also raises the question of "to aggregate, or not to aggregate". If we leave the teaching of cybersecurity practice in diverse places on campus, we are not going to be able to coordinate the message, let alone evolve the field into a mature discipline. However, if we pull all of the cybersecurity education into a single place that begs the question of "where should we put it?", since engineers will not be comfortable in a law school and vice versa.

The term "holistic" has been used to describe what has to happen in order for the solution to be complete and correct. But the problem is that most present faculty members specialise in some vertical aspect of the discipline of computing. They are not going to just drop what they are teaching and start approaching things holistically. So, a new breed of professional will have to be educated. That returns us to the question of what to teach.

It should be obvious that a broad-scale development strategy based on a comprehensive definition of the field is needed to address the problem. That strategy should ensure that the right learning experiences are provided to the right people, across the educational landscape. However, effective strategy requires understanding the status of the existing landscape. Current cybersecurity teaching encompasses three classic domains. Those are, in order of formality, Awareness, Training and Education. A fourth area is the Research activity that supports all domains. Each domain can involve systematic, curricular or programmatic schemes, as well as unsystematic, "ad-hoc" efforts. Finally, there are a range of communities of interest where security teaching and learning might apply. Those 17 settings are listed in the table at the end of this article.

Awareness can be both programmatic and ad-hoc. Awareness is a very useful mode of content delivery in that it can ensure a minimum level of correct practice among a wide range of people. Formal awareness programs such as DHS Stop-Think-Connect utilise established methods for disseminating general knowledge such as posters, presentations and commercials. Informal programs include any educational activity sponsored by an organisation or group. The practices themselves can be relatively simple, such as secure housekeeping, phishing avoidance, or secure passwords. The messages themselves are often boiled down to slogans or sound bites.

Training can be formally sponsored, even certified. Training can be formal or organised to address a specific problem. Training is focused on the acquisition of a particular skill. That skill can be complex, like network administration, or secure programming. But training is always time sensitive in that the skills being provided can be made obsolete by change. Formal training programs, particularly those associated with certification, are based on commonly accepted bodies of knowledge. The end result of a training program is demonstrated mastery of that body of knowledge. Ad-hoc training provides mastery of a skill that might be required for a given application, or setting. Ad-hoc training is often deployed as corrective action, or in order to plug a knowledge gap in a particular instance.

Education can be programmatic and curricular, or it can be general. Programmatic education seeks to provide a reasoned understanding of a discipline or field. That understanding must be comprehensive in that the individual is capable of developing a heuristic solution from a given set of facts. Education is not time sensitive in that the educated individual should be capable of applying existing knowledge by extension to new problems. Because that capability often requires acquisition of a large amount of knowledge, programmatic education is decomposed into logical elements. This collection of elements is normally called a "curriculum". General education is not discipline specific. It can display the same characteristics of curriculum-based education in that it provides comprehensive and extensible understanding. However, general education is not directed toward mastery of a particular field.

Finally, Awareness, Training and Education activity is supported by research. Research develops knowledge and refines practice. There are two types of research programs. The first is practitioner-based research, aimed at developing useful skills and techniques. The second type of research is scientific in that it generates and confirms the correctness of new knowledge. This type of research can be unapplied but it is valuable because it forms the basis for the principles of the field.

If the aim is comprehensive cybersecurity then some form of all of these teaching modalities is required in all of the classic areas of society, government, industry and academia. Because the cultures of each of these communities are so different, the awareness, training and education needs vary across communities. That is an important point to keep in mind in developing any strategy aimed at ensuring cybersecurity. That is because content in any modality must be tailored to the community of practice in order to be effective. The table below shows all of the modalities we have discussed arrayed against the 17 logical communities of practice.

The question is, "How much of this table is blank?" In order for information system security to become a mature discipline every cell in this table should have some activity taking place within it or a reasonable justification for why that is not happening. Looking at this table it is hard not to conclude that we have a considerable way to go before we can say that we have gained control over the problem. It also tends to reinforce the conclusions of the National Academy of Science's findings, which is that the field is still immature.

Daniel P Shoemaker, PhD, Principal Investigator and Senior Research Scientist at UDM's Center for Cyber Security and Intelligence Studies. This Center includes the Computer Information Systems-Information Assurance Department, as well as the NSA Center of Academic Excellence in Information Assurance Education. As the Co-Chair for the DHS National Workforce Training and Education Initiative for Software and Supply Chain Assurance, he is one of the three Authors of the Software Assurance Common Body of Knowledge (CBK).

	Research Practitioner	Research Theorectical	Education Curricular	Education Ad-Hoc	Training Program	Training Ad-Hoc	Awareness Program	Awareness Ad-Hoc
GOVERNMENT								
National Security								
Conventional Agencies								
Contractors								
Aquisition								
INDUSTRY								
Government Supply Base								
Conventional Developers								
IT Sustainment								
Aquisition								
General Workforce								
INDUSTRY								
K-12								
Community Colleges								
Proprietary (for profit)								
College Undergraduate								
University Undergraduate								
College Graduate								
University Graduate								
Post Grad								