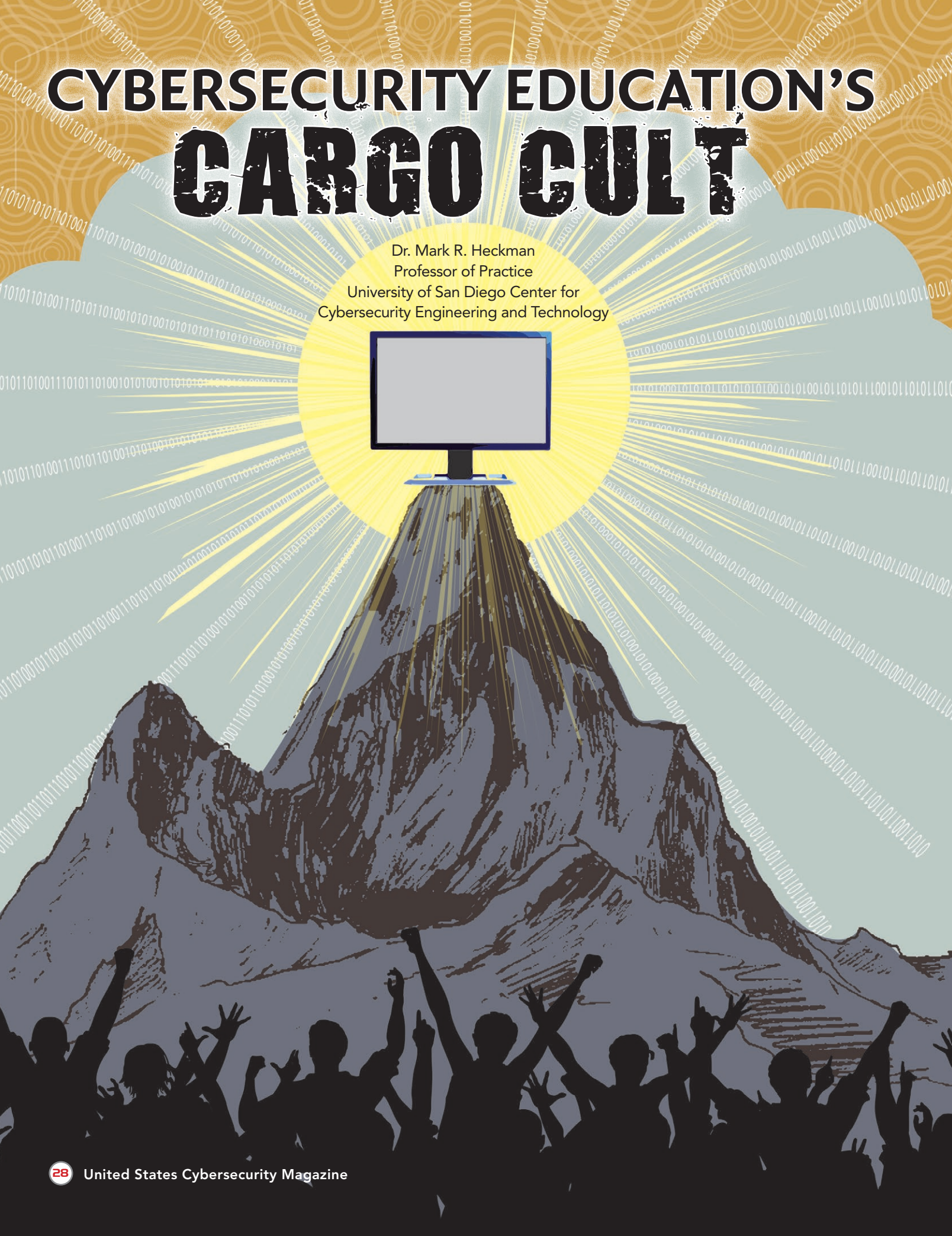
CYBERSECURITY EDUCATION'S CARGO CULT

Dr. Mark R. Heckman
Professor of Practice
University of San Diego Center for
Cybersecurity Engineering and Technology



During the Second World War, isolated island natives in the South Pacific observed how easily Allied military personnel based on the islands could obtain food and other supplies. The soldiers put on headsets, spoke into microphones, and airplanes soon appeared carrying the valuable cargo. When the war ended and the islanders were isolated once again, some of them attempted to obtain those supplies for themselves by mimicking the observed behaviors of the departed military personnel. The islanders did not understand the technology, but they believed they could succeed by building elaborate mockups of headsets, airfields, and even airplanes. They sat in fake control towers, spoke into fake microphones, and waited in vain for cargo planes to magically appear. Their beliefs gave birth to the term "cargo cult."

Since then, the cargo cult metaphor has been used to describe any efforts based on imitating the external form of something without understanding its substance. The physicist Richard Feynman, for example, famously used the term "cargo cult science" to describe pseudoscientific activities that mimic the external features of scientific experiments but lack the core attributes of the scientific method. A hallmark of science is continuing improvement in predictive range and accuracy; cargo cult science fails this test, but its acolytes explain away each failure and come up with yet another refinement. Feynman used the example of education methods to describe this particular aspect of cargo cult science:

> *There are big schools of reading methods and mathematics methods, and so forth, but if you notice, you'll see the reading scores keep going down--or hardly going up in spite of the fact that we continually use these same people to improve the methods. There's a witch doctor remedy that doesn't work. It ought to be looked into; how do they know that their method should work?*[1]

The field of cybersecurity has its own examples of cargo cult thinking. Standards and compliance, for example, have become the de facto basis for measuring security in organizations. But as any experienced cybersecurity professional knows, being compliant is not the same thing as being secure. Numerous studies show that the trend of cyber-attacks is increasing rapidly. Every year brings a greater number of increasingly severe and impactful attacks. Common prevention and detection techniques, layered on top of unsecure systems, have been largely shown to be ineffective. When compliant organizations are breached, however, analysis of the breach always finds some deficiency in the security practices of the organization that arose subsequent to the most recent audit, or else the auditing itself was found to be deficient. Target Corp., for example, passed a PCI audit not long before the massive hack of its point-of-sale systems was discovered. Both Target and its auditors were named in lawsuits for after-the-fact findings that Target was not, in fact, PCI-compliant.[2] But it isn't clear from forensic evidence that the memory-scraping software used by the attackers would have been addressed by PCI requirements.[3]

What evidence do we have that organizations would be secure if only they followed the standards better, or is satisfying the standards not enough to be secure? Most standards and other sets of "best practices" are ad hoc. They do not correspond to any formal model of security and very little in the way of controlled experiments have been performed to demonstrate their efficacy.[4] Instead, best practices typically consist of procedures developed through intuition and popularity. For example, ISO/IEC 21827, the System Security Engineering – Capability Maturity Model, "does not prescribe a particular process or sequence, but captures practices generally observed in industry."[5] Popularity is not a measure of effectiveness, yet standards and best practices, lacking proof as to their effectiveness, may be enforced with serious fines for non-compliance.

Even when certain practices can demonstrably improve security, the nuances of how and in what context they work are often lost when translated into an audit checklist. Organizations that focus only on passing audits and auditors who check the boxes are mimicking security practices without necessarily understanding how and why they function. Auditing based on standards typically verifies the outward form of a process, but not its substance. Satisfying standards and undergoing an audit becomes a form of ritualized behavior. Any expectation that organizations will be secure after simply passing an audit is magical thinking. These are the classic characteristics of a cargo cult.

The issue is not with standards and auditing, per se – there will always be a need to hold people and organizations accountable – but with how standards and auditing regimes foster blind efforts to apply security practices without an understanding of fundamental security principles and of the context necessary for those security practices to be effective. The result is misplaced confidence in the security of compliant systems.

To be fair to security practitioners, security is rarely the organizational mission and may sometimes be perceived as interfering with carrying out that mission. Moreover, security is expensive and the benefits are difficult to measure; it is much, much easier to measure the costs of a failure of security, but the incremental benefit of a particular security practice or mechanism is almost impossible to quantify. Security practitioners, with limited resources and limited ability, if any, to enact changes, must protect systems and networks that were developed without security in mind. Compliance is all they are allowed to enforce because it is the only way that they and their management can limit the costs.

Recent headlines shout about the severe shortage of skilled cybersecurity workers. The shortage is especially acute in what the U.S. Department of Homeland Security (DHS) calls "mission-critical" cybersecurity jobs. Faced with the ever-increasing number and severity of attacks, the need to protect highly vulnerable systems and networks, and the ineffectiveness of common prevention and detection techniques, the natural tendency of organizations is to seek people experienced in penetration testing (to try to find vulnerabilities before attackers do) and breach detection and incident handling (to manage the ever-increasing number of successful attacks). This tendency is exemplified by a 2012 DHS "CyberSkills Task Force Report," which listed the following as mission-critical cybersecurity jobs:

1. **System and network penetration tester**
2. **Application penetration tester**
3. **Security monitoring and event analysis**
4. **Incident responder in-depth**
5. **Threat analyst/Counter-intelligence analyst**
6. **Risk assessment engineers**
7. **Advanced forensics analysts for law enforcement**
8. **Secure coders and code reviewers**
9. **Security engineers-operations**
10. **Security engineers/architects for building security in**[6]

A more recent Council on CyberSecurity study funded by the Air Force Research Laboratory essentially reiterated this list.[7]

It is clear from the top five jobs in the list that the DHS sees discovering vulnerabilities and reacting to breaches as the greatest cybersecurity needs. But testing, even focused penetration testing, cannot possibly find all of the vulnerabilities in systems, and even the most skilled intrusion responders, by definition, will always be playing catchup to attackers. Furthermore, if penetration testing and incident handling are so desperately needed, this is a de facto admission that a system is not secure.

But where is the proof that hiring more people with these skills will improve security? Are there any fully staffed, successful examples? If these jobs are not, in fact, mission-critical, then training and hiring more people to do them will not improve security, and may even harm security by drawing resources away from other, more effective security activities. Once again, we have a situation in cybersecurity where practices (in this case, security training practices) are being promoted without sufficient evidence that they are effective. There is ritual in the form of training and hiring, and magical thinking that the result will be greater security. There is, in other words, a cybersecurity education cargo cult.

This is not to denigrate the need for highly skilled technicians; cybersecurity workers must have strong practical skills to be effective in their work. The criticism here is of the particular emphasis on reactive security jobs and the complete focus on practical skills without basing them on a foundation of fundamental security principles. This situation is strongly reminiscent of the story of the blind men and the elephant, where several blind men surround an elephant and describe what they think an elephant is. The man who touches the leg says the elephant is round and tall like a tree; the man who touches the tail says the elephant is skinny and flexible; and so on. Each blind man only knows what he can touch. While they are all partially correct, they miss the big picture. The same risk occurs with a cybersecurity workforce that consists of only narrowly trained technicians. They will each understand their own specialty, but not necessarily what it takes to make a system secure.

A recent RAND report notes that advances in secure architectures could make the top five mission-critical jobs obsolete. Those skills are needed because the current dominant computer system architecture permits malware. Eliminating the problem of malware would not by itself lead to perfect security, the report says, but it could reduce most of the process of keeping systems secure to "administrative housework," which does not require the same level of training. "The current concern over cybersecurity could easily abate, driven by new technology and more secure architectures. Pushing too many people into the profession

now could leave an overabundance of highly trained and narrowly skilled individuals."[8]

It is a widely accepted principle in cybersecurity that the best way to create secure systems is to build security in from the very beginning and not depend on mechanisms and processes layered around an unsecure system. Yet languishing in eighth and tenth place in the DHS list, respectively, are "Secure coders and code reviewers" and "Security engineers/architects for building security in." A 2010 Center for Strategic & International Studies (CSIS) white paper, on the other hand, said, "We not only have a shortage of the highly technically skilled people required to operate and support systems already deployed, but also an even more desperate shortage of people who can design secure systems, write safe computer code, and create the ever more sophisticated tools needed to prevent, detect, mitigate and reconstitute from damage due to system failures and malicious acts" (emphasis added).[9] To improve security, the CSIS paper suggests, the greatest need is not for narrowly trained specialists in reactive security jobs, but for engineers trained to design and build secure systems and the tools necessary to keep them secure.

The field of cybersecurity has a proven set of foundational principles, the development of which began over 40 years ago. Many of the problems we face in cybersecurity today were first identified, and solutions proposed, in the 1970 "Ware Report"[10] and the 1972 "Anderson Report,"[11] for example, but their findings and conclusions are rarely, if ever, taught to new security practitioners, and we continue to face the same security problems.[12] Security practitioners should be able to draw from knowledge of these foundational security principles as well as from systems engineering, software engineering, operational security, and supply chain security in order to develop processes, tools, and measures to effectively protect digital information. There must be a model of security that underlies and connects specific practices and mechanisms so that security becomes an integrated field rather than an ad hoc set of best practices. In other words, security should be practiced as a field of engineering.

As with standards and auditing, there will always be a need for skilled technicians. But technicians generally follow processes created by engineers, using measures and tools created by engineers. And while specialized technical skills can quickly become obsolete, training in fundamentals is useful no matter how technology changes in the future. The emphasis on cybersecurity education must not be on an unproven, panicked response to a short-term problem, but on what will effectively help make our systems secure in the long term. It's too important a task to leave in the hands of a cargo cult.

Sources

1. "Cargo Cult Science", by Richard P. Feynman, June 1974 http://resolver.caltech.edu/CaltechES:37.7.CargoCult
2. Schwartz, M.J., "Target, PCI Auditor Trustwave Sued by Banks", 26 March 2014 http://www.darkreading.com/risk/compliance/target-pci-auditor-trustwave-sued-by-banks/d/d-id/1127936
3. Litan, A., "How PCI failed Target and U.S. Consumers", 20 January 2014 http://blogs.gartner.com/avivah-litan/2014/01/20/how-pci-failed-target-and-u-s-consumers/
4. Admittedly, controlled experimentation in cybersecurity is a very difficult proposition. See, for example, Pfleeger, S.L.; Cunningham, R.K., "Why Measuring Security Is Hard," in Security & Privacy, IEEE , vol.8, no.4, pp.46-54, July-Aug. 2010
5. http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=44716
6. President's Homeland Security Advisory Council (U.S.). CyberSkills Task Force. CyberSkills Task Force Report. [Washington, D.C.] : Dept. of Homeland Security, Homeland Security Advisory Council, CyberSkills Task Force, 2012 https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf
7. Lute, J.; Durrance, D.; Uenuma, M., Mission Critical CyberSecurity Functions. Council on CyberSecurity, February, 2014. https://www.cisecurity.org/workforce/img/MissionCritical.pdf
8. Libicki, M.C., Senty, D., and Pollak, J. Hackers Wanted: An Examination of the Cybersecurity Labor Market. Santa Monica, CA: RAND Corporation, 2014. http://www.rand.org/pubs/research_reports/RR430
9. A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters. White paper, CSIS Commission on Cybersecurity for the 44th Presidency. Center for Strategic & International Studies, July 2010 http://csis.org/files/publication/100720_Lewis_HumanCapital_WEB_BlkWhteVersion.pdf
10. Ware, W., ed. Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security, Rand Report R609-1 (Feb. 1970). Reissued October 1979. http://www.rand.org/pubs/reports/R609-1/index2.html
11. Anderson, J. P., Computer Security Technology Planning Study, ESD-TR-73-51, ESD/AFSC, Hanscom AFB, Bedford, MA (Oct. 1972) http://csrc.nist.gov/publications/history/ande72.pdf
12. For one approach to incorporating fundamental security properties in a cybersecurity curriculum, see Irvine, C.E., "The reference monitor concept as a unifying principle in computer security education", in Proceeding IFIP TC11 WC11.8 First World Conference on INFOSEC Education, Kista, Sweden, pp. 27-37, June 1999 http://calhoun.nps.edu/handle/10945/7200?show=full

About the Author:

Mark Heckman *has worked in the field of information security for over 30 years as an engineer, researcher, practitioner, and educator. His experience includes multi-level secure systems used by the military, intrusion detection and security event management systems, and IT security and compliance for commercial organizations in the financial and health industries. Heckman earned his Ph.D. in Computer Science at the University of California, Davis and is a Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA).*

University of San Diego