SEVEN OVERLAPPING THESES
ON CYBER-SECURITY EDUCATION

Scott Borg
Director and Chief Economist
U.S. Cyber Consequences Unit
scott.borg@usccu.us

The majority of the leading figures in real-world cyber security did not become the acknowledged masters of the field *despite* their unconventional and diverse academic backgrounds; they became the acknowledged masters *because* of their unconventional and diverse backgrounds. Entering the field of cyber security before there were regular university programs or even courses in the subject was actually an advantage. The current formalization of cyber-security training is in danger of actively *preventing* people from developing many of the skills and abilities that the field most needs. What's more, many of the proposals for improving cyber-security education would only make things worse.

The following seven theses are all essentially an elaboration of this point. They are based on many years of intensive, practical experience in cyber security, including in-depth, on-site investigations of nearly all the critical infrastructure industries. There wasn't room to describe the relevant experiences in this short paper. Most people with extensive practical experience in cyber security, however, will be able to think of many anecdotes that would support these seven theses.

Obviously, we need formal cyber-security training. We need far more practioners than could ever be produced or find their way into the field without regular academic programs. But we need to be sure that those programs are preserving at least some of the features that made many of the pioneering people in the field so adept and so innovative. We need to be sure we are preparing people not just for entry level jobs, but for future leadership roles. We especially need to be sure that we are not doing things in our training programs that put our graduates at a disadvantage when it come to dealing with highly creative adversaries.

Thesis One: An over-emphasis on STEM training is often making students *less* equipped to do cyber security well. The subject matter of natural science, engineering, and math, can be predicted by extrapolating from past cases. As Einstein famously said, nature is subtle, but it is not malicious. The uncertainties in natural science can usually be modeled by normal distributions. The subject matter of cyber security is not like that. Cyber attacks, their practical consequences, and the ways they can be foiled cannot be predicted by extrapolating from past cases. Cyber-security practitioners regularly need to deal with phenomena that are not just subtle, but malicious and cunningly so. The uncertainties in the field can hardly ever be accurately modeled as normal distributions. The often dazzling creativity of cyber attackers needs to be met with equally dazzling creativity on the part of defenders. When systems are under attack, defensive actions often need to be taken based on an intuitive assessment of what is going on, with no time for a comprehensive, carefully reasoned analysis, testing, or verification. Yet at the same time, the field is so open-ended, there is no objective way to put a limit on the facts that need to be taken into account. The whole mindset of natural science, engineering, and math is therefore profoundly wrong for doing cyber security.

Thesis Two: The information assurance triad of availability, confidentiality, and integrity, which still dominates cyber-security education, is obsolete as the goal for cyber security. This is because these categories describe features of information systems and cause defenders to focus on their own technology, rather than on potential attackers. The goal of cyber security should be to reduce risk, defined as annualized expected loss. The way to do this is usually to increase attacker costs. This means that the focus, even at a very basic, practical level, should be on stopping the things that attackers need to do in order to make their attacks pay off. Cyber security practitioners, guided by the information assurance triad, can rarely describe with any accuracy more than one or two components of what they are trying to prevent. Many of the most notorious cyber-security failures over the last several years can be traced to this failure in understanding.

Thesis Three: The *majority* of the topics cyber-security professionals most need to master in order to assess and reduce cyber risk are *not* covered in the curricula of most university cyber-security programs. This is partly because they are not included in the (ISC)^2 Common Body of Knowledge used for the CISSP exam, the NIST Cybersecurity Framework, or the other documents regarded by academics as defining the field. As a result, most cyber-security education focuses overwhelmingly on a narrow technical portion of the Vulnerability factor in the cyber-security risk equation. It largely ignores the other two factors in the risk equation: Consequence and Threat. When cyber-security programs pretend to address these other factors, they usually define them in a way that reduces them to aspects of Vulnerability. Despite the fact that economic factors drive almost everything that happens in cyber security, most cyber-security programs omit economics altogether. Even the specializations in cyber-security education are focused the wrong subjects. If cyber security is going to reduce risk, it needs to tailor its practices to the different economic and safety requirements of different industries. Yet cyber-security specializations are rarely organized by industry. Instead, the usual specializations regularly separate issues that, in practice, need to be handled together and by the same person. The NICE Framework, for example, puts many tasks into different work roles and different specialty areas that should never be performed by different people. Meanwhile, this same NICE Framework fails to distinguish between the very different cyber-security requirements of industries as distinct as railways, electronic manufacturing, healthcare, and financial services. At both a basic and an advanced specialist level, expecting cyber-security practitioners to protect industry systems without any genuine understanding of what those systems actually do, technically and economically, is a very bad educational strategy.

Thesis Four: The qualification hurdles designed to make sure that cyber-security professionals cannot get accredited without the types of expertise deemed most essential are effectively *excluding* the kinds of skills and expertise that are *really* most essential. Cyber security does not need practitioners who will faithfully do exactly what they were taught in school nearly as much as it needs people who can tackle a subject without being told what to do. It does not need people who can remember exactly what they were taught nearly as much as it needs people who can continually re-think things, and who can move across different disciplines so casually that they are barely aware of doing so. Before there were university departments in computer engineering, programmers were typically recruited from language departments, philosophy departments, linguistics departments, and even music departments. The broader liberal arts background associated with those fields of study was often more valuable for their later work than any specific training they received in matters relating to computers.

Thesis Five: The effort to make the study of computers and programming academically respectable, by describing it as a "science," rather than as a field of engineering, and by emphasizing mathematics, especially the mathematics of analog physics, has caused adverse effects on cyber-security education that urgently need to be corrected. Hardly any of the mathematics computer engineering students are required to learn is of any practical use in practical programming, let alone cyber security. This means that the math requirements in computer engineering and cyber-security programs severely limit the available talent pool without delivering any compensating benefits. Worse, treating computer engineering as though it were a science to be pursued for science's sake results in graduates who design programs and systems that are too fragile for the real world. It is as though engineers were being taught to design bridges "for bridge's sake," without ever having to worry about things like traffic, winds, earth tremors, metal fatigue, temperature changes, and future uses. Companies often have to train "computer science" graduates from our best universities for an additional year-and-a-half to two years before they can use them for anything important. Even then, these graduates tend to retain work habits that are not conducive to things like secure programming.

Thesis Six: Where cyber security is concerned, cultural diversity is not a laudable social goal, but a *functional* necessity, and, even though most educational programs for cyber-security education pretend to encourage this diversity, they actually go to great lengths to eliminate it. One of the ways educational programs do this is by assuming that the correct answer to almost every problem or test question will be same for every student. Real-world cyber security, however, depends on people seeing things differently, especially seeing things other people have missed, not only different ways of accomplishing the same things, but different things that could be accomplished. Cyber-security training should be encouraging and rewarding students who can come up with a *different* answer than anyone else. This is the opposite of current practice.

Thesis Seven: The technical jargon currently used in the profession and in many cyber-security courses is an obstacle to good cyber-security education. This is not primarily because of the barriers it puts between cyber-security professionals and the general public, but because it is riddled with fallacious assumptions, obsolete distinctions, category confusions, and usages inconsistent with better established disciplines. The terms used to describe cyber attacks, for example, do not follow any consistent principle. Some terms refer to propagation mechanisms, some to hiding places, some to activation times, some to attacker goals, some to technical effects, some to business effects, and so on, through at least sixteen principles of classification. The definitions cyber-security authorities, such as NIST, give for basic business and financial terms, such as “asset” and “risk,” are often simply wrong. What’s more, students tend to learn the technical terms, instead of the underlying concepts, and then get even the technical terms wrong. Despite these problems, most cyber-security programs, instead of making stringent efforts to avoid the jargon, pride themselves on teaching it. This has the further effect of making most cyber-security graduates incapable of defending their budgets when they are talking with senior business executives.

Scott Borg is Director and Chief Economist of the U.S. Cyber Consequences Unit, an independent, nonprofit research institute that investigates the strategic and economic consequences of cyber attacks. He is the leading authority on the economics of cyber security as well as a number of technical topics. He has been the principal proponent of a quantitative, risk-based approach to cyber security for nearly twenty years and is responsible for many of the concepts that are currently used to understand the effects of cyber attacks in business contexts. He is author of The ISA Guidelines for Securing the Electronic Supply Chain, the most comprehensive reference document for protecting electronics manufacturing. Along with John Bumgarner, he is co-author of the new US-CCU Cyber-Security Matrix, a complete survey of genuinely useful cyber defense measures, more than a thousand items long, organized according to the attacker activities they are designed to prevent. His other technical contributions have included pioneering work on the techniques for hiding and finding malware and new methods for analyzing it. Partly because of the way he has been able to employ economic models, his record for anticipating new developments in cyber security since 2002 is probably unequaled. He was able to predict Stuxnet, for example, its exact target, and exactly how it would reach and damage that target, fourteen months before it as found. He has been quoted in most of the world's leading news publications, comments for NBC, CNN, the BBC, NPR and other broadcast media, served on the Commission on Cybersecurity for the 44th Presidency, and has lectured at Harvard, Columbia, Berlin (Freie), and other leading universities. His current research is on the implications of cyber security for international relations.