Cybersecurity, by its very nature, is people—both defenders and attackers—engaged in a contest playing out on a field of information systems and technology. Just as in any contest of this kind, success lies in identifying talent and continually developing and conditioning teams of professionals.

However, the US currently suffers from a general shortage of new-entry engineers and information security experts. We need such experts to fill existing positions and solve the emerging challenges that threaten our companies, government, infrastructure, and security:

The Computing Research Association (CRA) reports that the number of bachelor’s degrees in computer science ... fell 43% from 2003-04 to 2006-07 [and] the number of new CS majors in Fall 2007 was half the number [it was] in Fall 2000. [This] drop in enrollment is not consistent with the current and expected demand for IT jobs.... The Bureau of Labor indicates that of the five job categories expected to see the fastest growth [through] 2016, two (including the number-one category) are in the field of IT.1

We need to find a way to develop professionals who can build and manage secure, reliable digital infrastructures and effectively identify, mitigate, and plan for asymmetric and blended threats. Here, we present a new model for developing the next-generation cyberworkforce that combines assessments, simulations, customization, and support systems.

The Workforce Challenge
Government, industry, and academia largely agree that addressing the deficit of well-developed cybersecurity human resources has become a priority for organizations across the US. There’s broad recognition that this highly specialized but ill-defined workforce has suffered from underinvested educational pipelines and disjointed development programs.

Traditionally, it has taken many years to mature a cybersecurity professional’s knowledge, skills, and performance. Reaching peak performance requires years of accumulated IT knowledge enhanced by years of additional security experiences. In sum, this career progression can lead to a mastery of the skills needed for forensics, operational response, and risk management, ultimately enabling a seasoned information security expert to perform the highly skilled actions needed to protect critical systems from unanticipated, emerging, and impactful cyberthreats.

Advanced threats, such as the Stuxnet Worm, aren’t easily detected or defended against. Skilled security practitioners along with situational-aware users and operational staff on the front lines must detect the signatures and feints often created by these highly intelligent threats—particularly those, like Stuxnet, designed to surpass the target network’s engineered and deployed defenses.

Current workforce development strategies must consider the challenges inherent in this highly dynamic field. In particular,

- conventional backward-facing protection methods often assume predictable, static infrastructure, when the reality is a dynamic, fluid environment;
- asymmetric threats challenge traditional security methods and practices, demonstrating
the growing need for new and better practices and, more importantly, greater levels of expertise; and
• professionals are often constrained by organizational silos that can isolate expertise—a challenge exacerbated by the lack of defined roles and advanced collaboration skills.

Through years of experience, we’ve gained an appreciation for the importance of skilled and knowledgeable people. Although cyberdefense tactics, security architectures, and tools can help address many common threats, they’re insufficient when addressing adaptive, embedded, and interconnected threats. The best defense requires a well-developed workforce.

Developing and Assessing Talent
In the professional development discipline, talent is frequently defined by three components: knowledge, skill, and ability. Often these terms are used interchangeably, but research has shown that expert performance reliant on skills (an observable psychomotor act) is notably different from entry-level performance by journeymen or apprentices, which principally relies on knowledge (a body of information applied directly to the performance of a function).²

Specifically, demonstration of skill is characterized by rapid and consistent response, increased situational awareness, and resilience to uncertainty, distraction, and distress. It’s frequently reported that 10,000 hours of practice over 10 years can be required to gain this level of proficiency in a field. With a cybercommunity that’s just a decade or two old, few are likely to have mastered all aspects of the field. Thus, a primary challenge facing the nation is to increase the general capability of the workforce while reliably determining the level of expertise at an individual level.

Historically, attempts to assess skill have used questions of general cognitive knowledge and reasoning. These tests include college entrance exams, the Armed Services Vocational Aptitude Battery, and other achievement tests. However, studies have shown that these tests have very limited predictive validity and that skilled performance involves more than acquired knowledge of a task domain.⁴–⁷ Exciting developments in cognitive science are changing how we assess and measure skill, offering new algorithms and testing methods to better distinguish knowledge from skill.⁶–⁸–¹⁰ Applying these new theories to examination and assessment development will help distinguish those with expert-level expertise from those with intermediate-level expertise.

Researchers developed the ThinkLet theory of expertise, for example,⁶–⁸ in an effort to better measure and predict job performance. Early adaptation of the ThinkLet concept in group decision support software demonstrated an ability to create repeatable and predictable performance in individuals and teams.⁹ According to this research, skill develops after sufficient practice leads to the formation of neural clusters deep in the unconscious that execute behavioral programs without the need to recall specific instructions or procedures—the brain’s equivalent to a software applet.

Researchers have also recently developed new measurement methods. For example, potential performance analysis (PPA) can distinguish the use of knowledge recall from skilled performance and estimate ability, or potential performance, using an assessment of current knowledge and skills.¹⁰ Research based on PPA suggests that individuals performing tasks using knowledge alone are likely to see dramatic improvements as deliberate practice leads to skill formation over time.

Training and Simulating CyberThinkLets
These advances in cognitive science suggest a new approach to developing the cyberworkforce. As asymmetric and blended threats become the norm, the efficacy of practice in preparing for a response diminishes. Skilled personnel might risk using yesterday’s weapons to fight tomorrow’s war. Conversely, knowledgeable staff might be more adaptive but produce more errors and omissions in stressful, complex, and ambiguous environments. Certified expertise grounded in dated methods and tools could become a liability rather than an asset unless constantly refreshed to reflect the changing threat landscape. In other words, we need to infuse ground truths into our information assurance strategy. Ground truths refer to understanding how cyberattackers compromise systems—these “truths” comprise a working knowledge of the tactics, techniques, and procedures used by advanced or leading attackers. This knowledge helps us properly adjust security methods.

Airline pilots are trained using advanced simulators to deal with similarly difficult conditions and system failures. Applying this principle to cyber and information security would let security and operational staff experience low-frequency but high-consequence attacks against the systems they design, defend, and operate. Success of the US Cyber Challenge (www.uscyberchallenge.org) and
related programs at the secondary- and post-secondary school levels have shown the potential for using simulation to both develop and assess cybersecurity skills.

While such practice-intensive development solutions are urgently needed, the potential of each participant must be continually assessed and used to guide customized training programs to shorten learning curves. A workforce development program must be holistic in how it measures, develops, and supports cybersecurity expertise. It should

- address the human factors of accelerated expertise development (including book knowledge, hands-on skills, innate abilities, and cognitive and behavioral influences);
- focus on all phases of the end-to-end workforce development cycle (such as assessment, training, measurement and certification, retesting, professional development, and communities of practice);
- develop ground truth expertise, enabling professionals to “think like attackers” and integrate the changing landscape into how they design, build, deploy, and manage their environments; and
- define the ladder of expertise by distinguishing professionals at each stage of development and providing feedback at an individual level to aid in professional development.

Given this need to develop and grow a strong information security workforce in the US, we’re in need of a new roadmap for success.

Developing Security Experts
Researchers at the National Board of Information Security Examiners created the Ground Truth Expertise Development model, which is based on the following (see Figure 1):

- a detailed understanding of job requirements;
- multidimensional aptitude assessments;
- customized training and simulation;
- knowledge and performance-based measurement of skills;
- personal development plans for continual development; and
- the use of performance support systems and simulation to continually refresh these skills based on ground truths.

Using the Ground Truth Expertise Development roadmap to identify and develop world-class security experts should help the industry develop, replicate, and continually enhance best practices.

Solving the US’s cybersecurity challenges will require all sectors to systematically learn about weaknesses; identify and understand new threats; and make better design, deployment, and operations decisions. The time is now to develop our greatest resource in this contest—the professionals who defend, operate, and protect our critical systems and infrastructure. As President Obama noted in May 2009,

From now on, our digital infrastructure—the networks and computers we depend on every day—will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage.11

![Figure 1. The Ground Truth Expertise Development cycle. This model can help identify and develop world-class security experts.](image-url)
From a professional’s perspective, effective security and response to advanced cyberthreats requires

- a current understanding of what adversaries are capable of,
- an opportunity to experience directed attacks to become familiar with observables and experiment with response actions, and
- a team training framework to optimize defender tactics, techniques, and procedures.

Customized training systems must adapt to individual skill profiles and accelerate skill development to let professionals practice defending against simulated attacks. By instilling ground truth, threats that have traditionally been hypothetical can be made real for learning and preparation purposes. It’s time to more formally assess and prepare our frontline defenders to ensure they’re competent, prepared, and capable of making the right decisions day-to-day and during emergencies, despite the distraction or distress created by a constantly shifting adversarial threat.

To achieve resilience in an era of dynamic and adaptive threats, security professionals can’t rely solely on book knowledge. No matter how good the protection systems are, there’s little doubt that the best preventive measures will be compromised in some way by cyberthreats in the future. Given this reality, conventional “certified” practices and protections aren’t enough.

The proposed Ground Truth Expertise Development model uses the latest advances in psychological, cognitive, and social science to identify and develop security “top guns” who can work productively under pressure, think together creatively, regroup adaptively, and adjust swiftly to any tactical failures to create a resilient systems security architecture.

References

Michael J. Assante is president and CEO of the National Board of Information Security Examiners (NBISE). His research interests include high-impact, low-frequency risk; threat management; and workforce development. Assante received his BA in political science from Miami University at Oxford, Ohio. Contact him at michael.assante@nbise.org.

David H. Tobey is chief scientist of the National Board of Information Security Examiners (NBISE). His research interests include expertise and skill identification, development, and replication. Tobey received his PhD in business administration from New Mexico State University. Contact him at david.tobey@nbise.org.