[in]security

by Gary McGraw

Are We In a Computer Security Renaissance? : : :

I believe we're experiencing a time of great creativity in computer security, in part because many experts come from outside the security discipline. Many of today's security practitioners were trained in fields as diverse as biostatistics, divinity, economics, and cognitive science. This diversity brings interesting new perspectives to the security challenge and leads to creative interplay that results in forward progress. We've seen evidence of this in the emergence of economic theories of security, the rise of risk management and security engineering, and a shift toward process-driven approaches (vs. product sets) and software security.

Computer security used to be dominated by military and espionage-oriented research—think cryptography, code breaking, communications monitoring, and so on. But the widespread adoption of the Internet and e-commerce helped change the focus of security research. With money at stake, security quickly became as relevant to businesses as it was to training in some field of study. This means that as a collective, the computer security arena is filled with diverse and interesting points of view—exactly the sort of petri dish of ideas that led to the Renaissance at the end of the Dark Ages.

Having a diversity of ideas is healthy and lends creativity and drive to the security field. A great example is the new subfield of software security. Only five years ago, the notion that bad software might be a major root cause of security issues wasn't common. Today, we understand that programming flaws in OSs and applications can cause more exposure to threats than a poorly configured firewall.

TOMORROW'S TRAINING

These days, academic and professional programs are being put in place to train the next generation of security professionals. Soon, standard curriculums will be developed, and students will be required to understand the

> ❝ **Computer security must remain inclusive to retain its creativity.** ❞

national defense.

A number of young researchers joined the field in the mid-1990s, and this influx of "new blood" shook up the traditional security research community. For instance, the commercialization of the firewall, the rise of anti-virus technology, and the adoption of modern platforms such as Java and .NET were all spearheaded by new thinking in this area. As we continue to shift from guns, dogs, and concrete to networks, information systems, and computers, we must remember to take advantage of this creative diversity.

TODAY'S TRAINING

Only a handful of people working in computer security today started their careers in the field. In fact, academic programs expressly designed to train security practitioners are a recent phenomenon and remain rare.

Interestingly, this dearth of "qualified" people may be an asset. Though few practitioners have academic security training, they most assuredly have academic

same core set of concepts. This will certainly help to solidify the field of computer security, but at the same time there's a danger that generalization may lead to a homogenization of security. Instead of the creative soup afforded by a multiplicity of perspectives spanning many fields, security runs the risk of becoming staid and static.

On the other hand, if we're careful to avoid complete homogenization of the field, we can retain the benefits of diversity while building a solid academic discipline. One way to do this is to encourage those seeking computer security degrees to expand their study to supposedly unrelated disciplines. Another is to ensure that outside perspectives remain welcome. Computer security must remain inclusive to retain its creativity.

In any case, we must take advantage of the situation we find ourselves in now. We must pay close attention to different ideas, embrace change, and help security continue to evolve, even as it begins to crystallize.

↪ Gary McGraw is CTO of Cigital, a software quality management consultancy. He is co-author of *Exploiting Software* (Addison-Wesley, 2004), *Building Secure Software* (Addison-Wesley, 2001), and *Java Security* (Wiley, 1996). Reach him at gem@cigital.com.