Emerging Cyber Threats Call for a Change in the 'Deliver Now, Fix Later' Culture of Software Development

By Girish Seshagiri, CEO of Advanced Information Services Inc. (AIS)

The demand for new and innovative technology solutions has created a software industry laser focused on speed to market, costs and product functionality. While this may help companies achieve a first-to-market advantage, it has also led to an environment where developers are more focused on meeting unrealistic schedule commitments than producing high-quality software.

The result is a "deliver now, fix later" software development culture, where it is acceptable to leave the task of finding and fixing bugs until after the product has been delivered. Unfortunately, this has left software highly vulnerable to misuse by cyber criminals, hackers, and others, who are exploiting undetected defects to launch cyber attacks, steal intellectual property, and access other sensitive information.

According to a 2012 NSS Labs Vulnerability Threat Report, the number of software vulnerabilities tracked by the National Vulnerability Database is on the rise. 2012 saw a 26 percent year-over-year increase in reported vulnerabilities. In an interview with *eWEEK* about the findings, Stefan Frei, research director with NSS Labs, pointed to the fact that software managers and developers "have yet to come to grips with the secure programming techniques and processes necessary to permanently reduce the number of vulnerabilities found in their products."

Commit to Quality, Reduce Risk

Well-publicized software failures in recent times have been spectacular. We want these failures to become the exception instead of the norm. We want to encourage a thriving industry that easily enables quality work to happen.

But how can software developers meet market demand for products, without putting their software at risk?

Part of the challenge – and the solution – lies in recognizing and changing some of the practices around how software is bought and sold. There are three key areas that need to be addressed:

1. **Expect more –** Software buyers generally have minimal guidance on the level of quality they should expect, other than boilerplate quality-assurance plans. As a result, there is no demand or expectation for error-free software. Instead, buyers focus on meeting delivery deadlines, rather than insisting on a quality-assured product with a seller's guarantee – which could save them significant time and money. Buyers can – and should – expect more from their software vendors and not contribute to the "deliver now, fix later" attitude that has permeated the industry.
2. **Be responsible for quality –** Likewise, software vendors tend to resist providing quality guarantees on their work, opining that it would have a detrimental effect on project schedules and costs. What's more, poor quality often works in their favor, justifying additional revenue to fix problems with the software that could have been delivered right the first time.
3. **Empower software developers –** As an industry, we must recognize the need to build strong security practices into every aspect of the development cycle, not just as a bolt on fix after the fact. This means

"Well-publicized software failures in recent times have been spectacular. We want these failures to become the exception instead of the norm. We want to encourage a thriving industry that easily enables quality work to happen."

"As an industry, we need to recognize the need to build strong secure practices in every aspect of the development cycle, not just as a bolt on fix."

empowering software developers and teams with the proper skills and training so they can minimize the number of defects in their software and deliver products with fewer vulnerabilities the first time around. Certification organizations such as (ISC)²® are critical to the industry overall, because they are dedicated to raising the level of technical expertise and education of IT professionals. (ISC)²'s Certified Secure Software Lifecycle Professional (CSSLP) certification is specifically designed to instill software developers with the best secure software development practices and skills they need to combat the growing number of software threats and vulnerabilities.

Quality is our number one goal at Advanced Information Services (AIS). AIS provides software applications development, modernization and enhancement services. We are one of only 23 organizations in the U.S. whose software process is independently appraised at SEI CMMI® Maturity Level 5.

From the beginning, we have recognized the importance of high-quality software, building a global reputation for our secure coding practices and for consistently delivering nearly defect-free software with predictable costs and on schedule. We offer firm fixed-price contracting with performance guarantees, including a lifetime warranty on software defects. AIS teams practice effective defect management, comprehensive planning, and precise project tracking and reporting.

What this means to customers is a dramatically reduced number of security incidents attributable to poor quality software code. A great example of this is our recent work to help modernize a U.S. government agency's mission-critical legacy system – a project that was completed ahead of schedule.

AIS implemented the modernized system containing more than 680,000 lines of code, including the code to migrate one of the largest databases in the federal government. The AIS team delivered a high quality solution on time as evidenced by independent testing, which detected zero cyber security vulnerabilities in the code.

In addition to improved security, customers have been able to reduce software operations and maintenance costs by more than half. Instead of investing time and money to fix bugs in the production software, customers can reallocate that spend toward new features and enhancements.

"(ISC)²'s Certified Secure Software Lifecycle Professional (CSSLP) certification is specifically designed to instill software developers with the best secure software development practices and expertise they need to combat the growing number of software threats and vulnerabilities."

Software Quality: A Competitive Advantage

While time to market, cost and product functionality will always be important factors for success, it is increasingly evident in today's threat environment that a focus on quality will be a game changer for driving competitive advantage. The software companies leading the way will be those that make a commitment to quality from the boardroom on down. Likewise, buyers who demand quality guarantees as part of the seller's core deliverables will serve to foster a culture of quality and best practices. Finally, technically trained, quality-focused software developers are at the forefront of this movement. We need to support them with the skills, advanced certifications, and ongoing training they need to produce software that is not only innovative, but also secure.

Today software defects cost the government $10 to $15 billion per year, and the information assurance industry soon may amount to $1 trillion to protect against cyber attacks. We would all profit considerably if we could make the commitment to producing quality – from the beginning.

(ISC)² CSSLP