

United States House of Representatives  
House Armed Services  
Subcommittee on  
Terrorism and Unconventional Threats and Capabilities

Hearing on:

*Harnessing Small Businesses Innovation for National Security  
Cyber Needs*

Roger Thornton  
Founder and Chief Technology Officer

Fortify Software  
2215 Bridgepointe Pkwy, Suite 400  
San Mateo, CA 94404

July 28, 2010

**Testimony of Roger Thornton  
Founder and Chief Technology Officer**

**Fortify Software**

**San Mateo, CA  
July 28, 2010**

Good afternoon Chairwoman Sanchez, Ranking Member Miller, and distinguished members of the Committee. I appreciate this opportunity to comment on the crucial role of small business innovation within the realm of cyber security.

My name is Roger Thornton and I currently serve as the Chief Technology Officer at Fortify Software. I have worked in the Information Technology industry in Silicon Valley for the past twenty- three years. During that time I have been involved with the formation and development of over a dozen startup companies and have held engineering and management positions with some of the world's largest technology firms.

My technical expertise is in finding, fixing and preventing the software vulnerabilities that are at the very core of our cyber security dilemma. My current responsibilities involve the development and design of processes and technologies that eliminate software vulnerabilities in order to make IT systems resilient to the literally billions of attacks we see each day on the Internet – making software “hacker-proof” if you will. Traditional IT security strategies – the status quo – attempt to mask these underlying vulnerabilities with bolt-on security features and that approach has led us to the situation we find ourselves in today. The approach my firm has pioneered represents a fundamental shift in thinking as we have moved the security strategy from defending network perimeters and blocking attacks to hardening the core of our IT systems making them impervious to attacks – moving from network security to software security.

Fortify is a small company - a classic “Silicon Valley” startup - founded by myself and three co-founders in the spring of 2003. As with many innovative small businesses we have experienced rapid growth that has not just helped more than 700 customers transform their cyber security strategies, but has also created jobs and increased tax revenues within our communities. Today we employ over 200 people in 14 countries around the globe that help businesses and government agencies locate, eradicate, and prevent the software vulnerabilities that enable our adversaries to penetrate our most critical systems. Our customers include eight of the ten largest banks in the world, all the major branches of the US military, and a majority of the major telecommunications firms in the US and Europe, along with a host of other leading firms in the retail, insurance, healthcare, and manufacturing sectors.

Through the course of my work I am familiar with the amount and types of vulnerabilities found in our nation's most critical infrastructure and I can tell you with emphatic certainty that we are in a desperate situation. My firm's technologies have helped conduct audits on thousands of critical IT systems and not once have we found a system with no critical vulnerabilities - in most cases we find literally thousands of such issues.

One example set of data comes from a Fortify team that conducts audits and reviews of military systems. Over the course of two years that team has audited 601 software applications across 141 major programs and found over 3.8M security vulnerabilities – 441,813 defined as critical. This is not exceptional but has become the norm and represents a problem that is not currently receiving appropriate attention. Now of course, we help organizations eradicate these vulnerabilities as we find them, but for every system we have audited and remediated, there are a thousand others we have not yet engaged. And there are organizations that find thousands of critical vulnerabilities in their systems and due to funding constraints make a conscious decision to do nothing. Fortify is one of a few firms entirely dedicated to solving this problem.

There are two compelling reasons for you to consider and actively support the role that small businesses like Fortify have to play in solving cyber security issues.

The first is economic. Small businesses have historically been an incredibly important driver for job growth in the US economy and cyber security is no exception to that rule. According to the US Small Business Administration the estimated 29.6 million small businesses in the United States:

- Employ just over half of the country's private sector workforce
- Hire 40 percent of high tech workers, such as scientists, engineers and computer workers
- Represent 97.3 percent of all the exporters of goods
- Represent 99.7 percent of all employer firms

*Source: U.S. Small Business Administration Office of Advocacy, September 2009*

At the close of the first year Fortify was in business (2003), the Dow Jones Industrial average was at 10,453.92, this week it opened at 10,424.17 – the nation's largest companies have spent the last ten years treading water. Over the same timeframe, my company has seen a 1,500% growth in revenues and has added nearly 200 high-paying technology jobs to the US economy.

The second imperative for the active participation of small business in the domain of cyber security is their propensity to introduce much-needed, radical innovation into the marketplace.

The status quo for IT security has generated an extraordinary amount of profit in creating the unsustainably insecure environment we find ourselves in today. According to Gartner Group over the past five years the IT security spending in the US was nearly \$70B / year – this at a time when all branches of the US military and nearly every major company in America were victims of cybercrimes large and small. Only a small company would have the audacity and the impetus to challenge the status quo and offer an entirely new approach to a problem with entrenched solutions.

Like many small businesses, our company was founded on a simple observation that challenged conventional thinking. That observation led to a fundamental innovation – a radical departure from the status quo and in our case a complete change in the way we look at and solve the problem of cyber security, and that resulted in our success and growth.

Our observation was this:

1. IT systems are comprised of networks, hardware and software. Networks connect computers that have software programs running them.
2. The prevailing strategy for IT security is to “secure networks” by limiting access and attempting to block attacks as they happen.

3. That traditional cyber security approach has become outdated and is fundamentally flawed. It is a game we are destined to lose. Why? Simply put, nearly all the software we rely upon to run our critical infrastructure is built with major vulnerabilities – consider them effectively “open doors” for hackers. Our adversaries have shifted their approaches to leverage these “open doors” in software and we have responded with increased spend in the security of our networks. The results speak for themselves.
4. If we eradicate the software vulnerabilities the attacks won’t work – we can build our software systems to be resilient to attack. This is not much different from today’s practice of building office buildings that are resilient to fire.

This line of thinking represented a radical departure from the status quo and a complete change in the way we look at and solve the problem of cyber security – and in the Silicon Valley that means a new small business determined to solve an old problem in a new way. In spite of the strides we have made at Fortify and other small firms developing innovative cyber security solutions, the status quo still poses extraordinary challenges that could use your support to overcome.

These include:

1. **Disproportionate** focus on protecting Hardware and Networks while the majority of the attacks are at the Software Layer
2. **Lack of Policy** relating to software security that leads naturally to vague software security requirements and inadequate funding for software security initiatives
3. **Inadequate Funding** to fix the “holes” once they are found in legacy software programs
4. **Outsourcing of Mission Critical Software Development to Contractors** and third parties

As an industry, we have inadvertently developed our way into an unsustainable cyber security dilemma and only the most disruptive innovations will help us find our way out. The solutions to address this problem are almost certain to come from small, innovative companies. These small businesses have produced enormous economic prosperity for our nation and in this realm they will hold an extraordinary importance in our national security.

Allow me to frame the problem for you as we have observed it over the last seven years in greater detail.

Last summer a journalist asked the newly appointed Federal Chief Technology Officer, Aneesh Chopra, a typical question “What keeps you up at night?” The CTO responded with “it is not the recent denial of service attacks over the Fourth of July – but sloppy software implementations that have left holes open for hacking.” Hackers, all over the world, rely on these holes or vulnerabilities being left open so that they can easily penetrate systems operating in the US whether they are in the defense, financial, or critical infrastructure protection industries. We would submit, however, that it is less an issue of “sloppy software implementations” but more often a lack of awareness on how to build and maintain secure software. The ability to find and fix existing vulnerabilities in legacy systems as well as prevent additional vulnerabilities from being introduced into new developments has become part of the critical path to thwart the Advanced Persistent Threat that professional hackers hosted by nation-states have come to represent.

In the last year, we have witnessed an important evolution of thought represented by the draft cyber legislation from several committees that has elevated the focus on software to provide parity for software security. We were pleased to see the Armed Services Committee address the specific issue of software security in the Draft NDAA for FY2011 in Section 932. The language in Section 932 will advance America's long term security goals by transforming how the software industry and users approach security to deal with the growing threat of Cyber Warfare. Historically there has been a disproportionate focus on funding for hardware and network security. In the last ten years considerable sums of money have been spent specifically to bolster network defenses.

However when a critical breach occurs the refrain is not “my network was stolen”, instead the lament is typically “thousands of data records were stolen.” Ultimately the majority of these attacks have exploited vulnerabilities in the software layer that allowed them to access data. Industry analysts now estimate that up to 75% of attacks are attributable to the software layer. Our goal is to raise awareness on the necessity to harden the software layer as the last line of defense to protect critical systems and their data.

Select critical infrastructure industries have mandated adherence to software security principles. As an example the financial industry enacted the Payment Card Industry- Data Security Standards (PCI-DSS) requiring companies to analyze their software for known vulnerabilities, and to fix those vulnerabilities. The penalty for failing a PCI audit is strict – loss of the ability to process credit card transactions – and has contributed to stronger software systems and a reduction in overall exploitable vulnerabilities. Adoption of software security requirements outside of the financial industry is lagging; nevertheless, awareness of the problem is growing dramatically due to the spate of recent hacks that have been made public and the realization that the software layer is so vulnerable.

I’m sure you are aware of the publicity surrounding the Google hack in 2009, in which one of Google’s primary applications, Gmail, was hacked into ostensibly to spy on communications between Chinese human rights activists. Google was not the only company hacked. According to recent reports, over 30 other US-based companies were compromised, with the primary intent to gain access to software code repositories. There are two reasons to access source code repositories – either to steal intellectual property, or to modify the source code without the owner’s knowledge, perhaps inserting a backdoor for future use. But the main reason I draw attention to this issue is because it wasn’t a “network” breach – most networks are open for business everyday – rather the root cause was a software vulnerability that allowed the hackers to gain control and credentials on the target organization’s systems.

While the damage done to date by massive cyber espionage (of exploitable software code) is impossible to calculate from an economic and national security standpoint, we are facing even more pressing disasters if immediate actions are not taken to counter a host of cyber warfare scenarios, especially those targeting mission critical information systems.

The United States Government is struggling considerably with the issue of secure software due to some unique constraints that have evolved out of aggressive outsourcing of software development to contractors and third parties. There are only a few agencies in the U.S. Government that still employ their own in house software development organization – the Department of Veteran’s Affairs, Social Security Administration, Federal Aviation Administration and the Internal Revenue Service are examples of agencies who maintain in house software development. The majority of the Federal Government, including the Department of Defense and Intelligence Community, outsource much of their software development to Contractors. In many other critical infrastructure industries it is the exact opposite where 80% of their software development is performed internally and only 20% is outsourced.

We have witnessed that the industries that have more control over their software development are much more inclined to incorporate software security into their development efforts. This one key difference represents a significant delta in how securely software is developed and whether or not the final software deliverable is only implied to be secure or is actually devoid of known vulnerabilities. While it is unrealistic to expect the Government to swap the ratio, recognition of this fact should be taken into account in any new legislation seeking to improve software security.

Another key point to illustrate the unique struggle of the Federal Government is the reliance upon custom software development in support of mission critical systems as opposed using Commercial off the Shelf (COTS) technologies. Weapons systems, guidance systems, satellite systems, and UAV’s are all examples of custom coded software systems that have been publicly reported to be under constant attack by hackers. For example, it has been reported that the F35 program was penetrated and purportedly several terabytes of data were stolen. It is highly probable that vulnerabilities in the software layer were exploited to gain access to that significant amount of data.

A stronger defensive posture to improve the security of third party custom developed software is paramount to improving the overall defense of these mission critical systems. The Federal Government should not accept software from third parties that have known vulnerabilities within the code.

A lack of clearly defined software security policy has led to a lack of clearly defined software security requirements which translate into a lack of funding for software security being incorporated into major programs. Furthermore, when vulnerabilities are found in software, it is not easy to determine who is responsible for fixing the problem and paying for the fix – the Government Agency or the developer of the software. Due to this lack of clarity it has become common practice to try and find a waiver around the problem rather than remediate and fix the vulnerabilities.

In terms of successfully requiring software assurance, the private sector – and the financial community in particular – surpasses the public sector. Financial organizations must develop, maintain and regularly test secure systems and applications under the Payment Card Industry Data Security Standard. Those that fail risk losing their ability to do business or face audits and fines.

Despite overwhelming and long-known evidence that software security is essential to safeguard sensitive data, no federal mandates exist for software security similar to other IT security practices. Most organizations don't sufficiently implement software security under the current certification and accreditation (C&A) model the federal government currently requires for agencies and partners. No federal budgets to date have included specific language requiring software security or how to implement it.

The federal government has taken some small steps to require software assurance in the software development life cycle for products it creates and buys. The Federal Information Security Management Act of 2002 (FISMA), which sets out federal IT security C&A requirements, only generally mentions software security assurance as part of an overarching IT security strategy. Instead, the law focuses on ensuring agencies implement a broad array of Commercial Off-the-Shelf (COTS) technologies such as firewalls and antivirus – all built, and designed to protect, according to the “bolting on” security model. That model was appropriate in the days when FISMA was enacted, but a more advanced “baking in” model is now available, which removes the vulnerabilities in the application itself, thereby effectively weaving a “Kevlar vest” into the software.

FISMA's attendant guidance, NIST Special Publications 800-37 and 800-53, provides more specific information but still concentrates more on adding security technologies to defeat threats instead of ensuring federal systems don't contain vulnerabilities in the first place. The Department of Defense has even more demanding requirements through the DoD Information Assurance Certification and Accreditation Process (DIACAP), which defines levels of system priorities and defect rationalization all the way to the application vulnerability layer. While the process itself is broad in scope, encompassing the entire DoD “defense in depth” strategy, it stops just short of mandating automated source code scanning and fixing vulnerabilities in the core software assets running the entire Department!

Unfortunately, all these steps have been largely unsuccessful for many reasons. They have lacked funding for implementation and penalties for noncompliance. No requirements exist for automated code scans, remediation and active protection of running applications. Many government and industry experts have complained since FISMA was passed that it is a paper tiger that rewards completing compliance checklists more than actually improving IT security.

Because FISMA does not require software security directly, accompanying guidance or procurement language does not include sufficiently specific detail. That has translated into awarding individual “stove-piped” software security-related contracts that only include the appropriate level of detail for software security implementation, instead of having such language included in all IT security-related contracts.

In spite of the lack of clear policy direction there are several DOD organizations and Government Agencies that have adopted a pro-active stance vis-à-vis incorporating software security practices. The U.S. Air Force has established the Application Software Assurance Center of Excellence (ASACoE) in Montgomery, Alabama after a foreign adversary successfully attacked the Air Force's Military Assignments application and stole tens of thousands of personnel records.

The Air Force has amassed a compelling body of reusable vulnerability knowledge from assessing the software of 600 applications resident at 141 Program Management Offices. They have discovered 3.8 Million total software security issues and approximately 440,000 critical issues that require remediation. The software vulnerabilities discovered by the Air Force likely represents the current attack surface of software for a typical DOD installation. The valuable insight gained by the ASACoE should be used to strengthen software applications throughout the entire Department of Defense and could also assist the Department of Homeland Security among others.

The U.S. Army has taken the issue of software security a step further by conducting both assessments of their software and requiring remediation of the critical vulnerabilities that they discover during the process. The Army Data Center in Fairfield, California is a software hosting facility where they plan to assess the security of the software before they allow the software access to their networks. Software that is deemed too vulnerable will not be provided an authority to operate on the networks that they control thereby creating an important gate that the software must pass. This is a common practice throughout the Financial Community where it is imperative to keep vulnerable software away from their networks so that it does not compromise other connected systems.

The Department of Veteran's Affairs employs over two thousand software developers to build their systems. The VA has invested in an enterprise capability to build software security into their software development cycle from inception instead of bolting on security as an afterthought. The Healthcare industry has also become increasingly cognizant of the need for strong security due to HIPAA and privacy requirements that have driven their adoption of software security principles.

Funding obstacles have bedeviled each one of these organizations and prevented them from fully implementing a mature software security program in the timeframes that they desire. Lack of an overall Federal Policy relating to software security has led Program Managers to look to their own Agencies for policy direction or be left to try and implement it one by one on their own programs. This piecemeal approach has been ineffective at thwarting the advanced persistent threat attacks as the level of intensity and volume of cyber attacks continues to escalate.

After hearing this refrain from countless organizations we strongly support the direction that the Armed Services Committee has taken in the draft NDAA Section 932 on Software Security. We believe that the draft language adequately addresses the four key challenges that we have observed. Namely, it recognizes Software as a distinct challenge separate but equal to the challenges in securing Hardware and Networks. This is an admission of the key role that software plays today in all major custom built applications whether they are administrative personnel systems or highly advanced targeting and weapons systems.

Second, the language addresses establishing strong policy guidance for assuring software systems particularly for covered acquisition systems initially. We feel strongly that in time this positive guidance will naturally flow down into all systems that are worthy of these security protections.

Third, the language will help establish achievable and measurable requirements for incorporating software security requirements into new, but more importantly existing legacy systems, to limit their exposure to exploitation by attackers. The language makes it very clear, for the first time, that when software vulnerabilities are found they must be fixed. That is not the case today and it has obviously caused considerable chaos and left the United States extremely vulnerable to attack.

Lastly, it is essential that a funding mechanism be established to ensure that the principles of software security are implemented in a timely fashion so that we can create the best possible defense.

As a small, innovative technology start-up we spend a considerable amount of our time creating awareness of what the true problems are in the fight against cyber threat and which problems are currently addressable by today's technology offerings. We have a strong conviction and have established high confidence that the right combination of technology, human capital, and processes can combine to confront the Advanced Persistent Threat and ultimately prevent Cyber Warfare. We look to Congress to establish the top level strategic policy guidance for Cyber and we applaud Congress for being so active as this inspires not only the mature small companies, like Fortify, but it also gives hope to the next generation of innovators to invest.

On behalf of all of us at Fortify, I would like to heartily compliment this committee, as well as both the House and Senate Armed Services Committee, for the leadership that you have shown on addressing the issue of cyber security. We have been very impressed with the professionalism and tenacity of your staff's ability to break down a complex and technical issue so that they could fully comprehend the implications of software security, and you are truly performing groundbreaking work

I would like to personally thank Chairwoman Sanchez, Ranking Member Miller, and the members of the Subcommittee for holding this hearing on the impact of small business innovations on cyber security issues. Software security is a key facet of any attempt to protect critical systems and to secure the data stored within those systems. We look forward to working with you and the House Armed Services Committee to continue to make sure software security becomes a fundamental component of all federal cyber security efforts.

## **Roger Thornton**

### **Founder & Chief Technology Officer**

Roger Thornton founded Fortify Software in October 2002, convinced that information security required a fundamental shift in thinking - from a focus on the perimeter to a focus on the core - the software code itself. Incubated with acclaimed venture firm, Kleiner Perkins Caufield & Byers and recognized by Business 2.0' magazine as the "Smartest Start-Up for 2005", A Silicon Valley native, his career began at Cypress Semiconductor, the technology stalwart labeled "a quintessential entrepreneurial company" by The Wall Street Journal. At Cypress he was ultimately responsible for the development of the firm's renowned manufacturing planning systems. Roger earned his BS and MS degrees in Engineering with honors at San Jose State University. Roger consistently consults with several venture capital firms, corporate executives and government leaders on security, cyber security policy and emerging trends.

### **Fortify Software**

Software code has become the focus and ultimate target of cyber security exploitation. While the individuals and nations, who continue to excel at gaining access to systems software and data, have refined their ability to exploit the software that runs mission critical systems the policies to protect Government systems have not evolved to counter this advanced persistent threat. Fortify Software, the leader in Software Security Assurance, automates the ability to find vulnerabilities throughout millions of lines of code, and assists with the remediation of those vulnerabilities ultimately fortifying the software from attack. Fortify has been working closely with the AF, Army, OSD, IC, HASC and SASC to strengthen the guidance for Software Assurance in the DOD Certification and Accreditation process.