Software 2015: Situation Dire

Don O'Neill

The increasing dependence of industry and government on an immature software profession whose promise exceeds its delivery has become a source of risk that teeters at the tipping point. The convergence of software, national security and global competitiveness interactions and their fragile dependencies could unleash a destructive synergy of propagating and cascading effects. All this is happening while both industry and government continue as free-rider software users who lack both the ability and will to act.

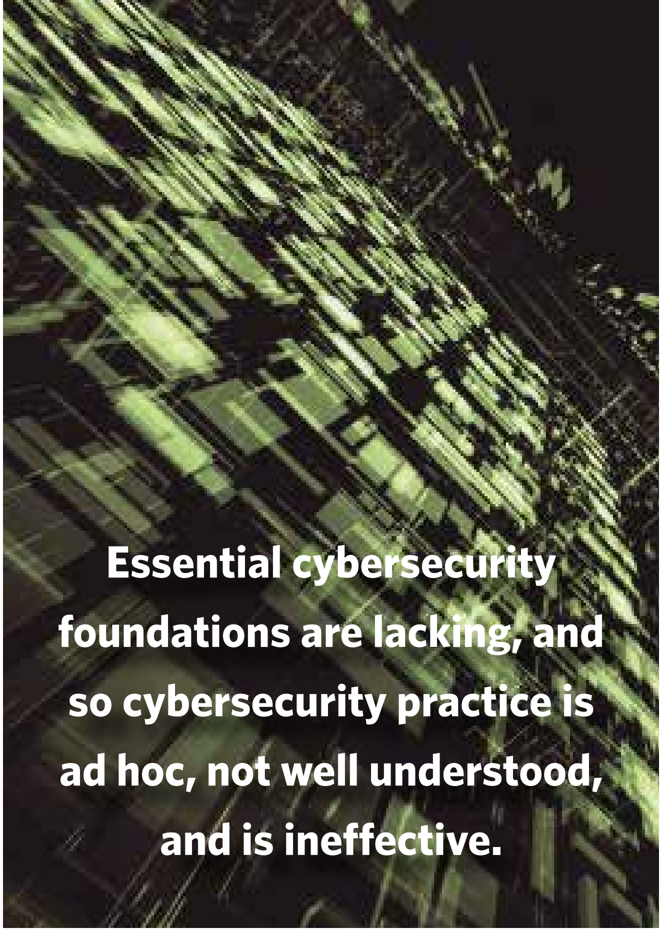
The Software 2015: A National Software Strategy to Ensure U.S. Security and Competitiveness—issued by the Center for National Software Studies in May 2005—observed that software is the critical infrastructure within the critical infrastructure, the theme of the Second National Software Summit (NSS2, 2005). The 2015 Software Vision was then stated as: "Achieving the ability to routinely develop trustworthy software products and systems, while ensuring the continued competitiveness of the U.S. Software industry," The question today is: Where do we stand with respect to the National Software Strategy and its programs? The answer is that the situation is dire.

Outcomes

The situation is dire in terms of National Software Strategy (NSS2, 2005) outcomes. Industry and government continue to increase dependence on software produced by an immature profession that has stumbled in delivering trustworthy software components, systems, and systems of systems to the nation's critical infrastructure and defense industrial base. This results in cybersecurity weaknesses and vulnerabilities that are exploited at will by persistent adversaries whose capabilities and motivation can only be surmised by assessing their consequences. A cybersecurity shortfall threatens competitiveness

O'Neill *was president of the Center for National Software Studies (CNSS) from 2005 to 2008. Following his 27-year career with IBM's Federal Systems Division (FSD), he completed a three-year residency at Carnegie Mellon University's Software Engineering Institute (SEI) under IBM's Technical Academic Career Program and has served as an SEI Visiting Scientist.*

0101110
0101101110101110
0101110
0101110



Essential cybersecurity foundations are lacking, and so cybersecurity practice is ad hoc, not well understood, and is ineffective.

by easy and continuing loss of intellectual capital to nation-states that drive on an information highway without rules or consequences.

Essential cybersecurity foundations are lacking, and so cybersecurity practice is ad hoc, not well understood, and is ineffective. Premature cybersecurity training and certification programs do not yield the capability to secure large-scale software-intensive systems, research programs are misdirected, Science, Technology, Engineering and Mathematics (STEM) initiatives promise what they cannot deliver, and executives and senior managers are disconnected from the realities they face. The increasing dependence on software to boost productivity and achieve competitiveness is not being met with increasing domestic workforce capability and capacity. Instead, enterprises in search of value continue to choose offshore outsourcing for skills and cheap labor despite vigorous political attempts to stigmatize this practice.

Citizen concerns about privacy, civil liberties and liability are obstacles to effective information sharing, and thereby erect barriers to achieving cybersecurity. While government dangles tax incentives, investment credits and insurance as incentives to purchase the full-throated cooperation of industry in information sharing, industry awaits a government offer of indemnification to unlock the stalemate and lubricate the risk calculations of critical infrastructure industry executives.

The nation's austerity and affordability challenges tied our hands just when the starter's gun signaled the beginning of the 21st century. On top of all this, the will to act is lacking due to a national leadership crisis.

Competitiveness

The most basic attribute of competitiveness is the sustainability of workers' wages. The Council on Competitiveness further states that competitiveness is the ability of U.S. products and services to meet the test of international markets while sustaining or boosting the wages of the workers who produce them.

Stages of competitiveness are organized around the activities associated with supplier control, customer control, competitor control, and event threat control. See Figure 1. Supplier control is achieved by establishing an attractive workplace culture, achieving maturity in process and skills, deepening industry relationships, and retaining personnel. The art of customer control is achieved by deepening customer relationships, balancing business factors, and achieving total customer satisfaction. Competition is controlled by deepening community relationships, fielding superior products, and setting the direction for the niche. Event threats and change are controlled by guarding against government intrusion, applying strategic software management, performing due diligence and understanding reality.

Numerous issues threaten competitiveness. The increasing dependence on software to achieve competitiveness is not being met with increasing domestic workforce capability and capacity. Enterprises in search of value continue to choose offshore outsourcing for skills and cheap labor. Cybersecurity shortfall threatens continued loss of intellectual capital. Tax policy, misguided regulations and antitrust litigation offer impediments and uncertainty. The austerity and affordability challenge ties our hands from the start. The Department of Defense (DoD), the defense industrial base, and the nation's critical infrastructure all face challenges in supply-chain risk

Figure 1. Competitiveness

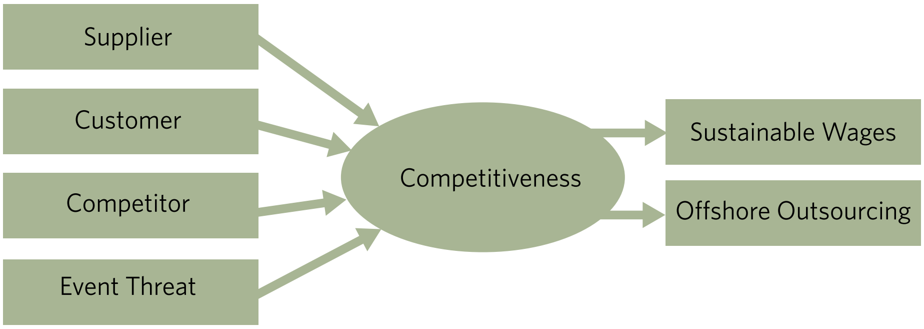


Figure 2. Security

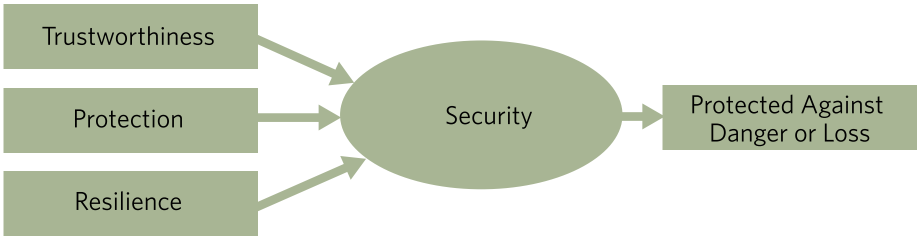
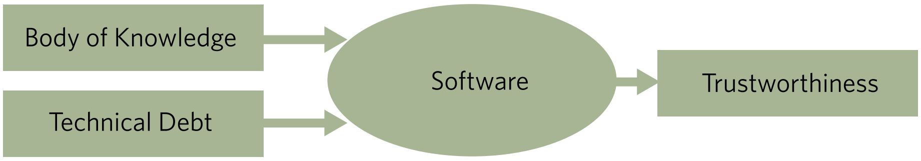


Figure 3. Software



management. These diverse challenges span infrastructure, trust, competitiveness and austerity. Beginning with acquisition, where supply chain foundations are laid, software and supply-chain risk management (SSCRM) assurance extends into operations and sustainment.

Security

The most essential attributes of security are trustworthiness, protection and resilience. See Figure 2. Security is defined as being protected against danger or loss. Software assurance is the level of confidence that software is free from vulnerabilities. It involves trustworthiness and no exploitable vulnerability, justifiable confidence in predictable execution, and conformance through planned and systematic multidisciplinary activities.

Simply put, the goal of cybersecurity is to assure the trustworthiness, security and resiliency of software components, systems and systems of systems of all kinds, including those used in national defense and the nation's critical infrastructure. Resilience is the ability to anticipate, avoid, withstand, mitigate and recover from the effects of adversity, whether natural or man made, under all circumstances of use.

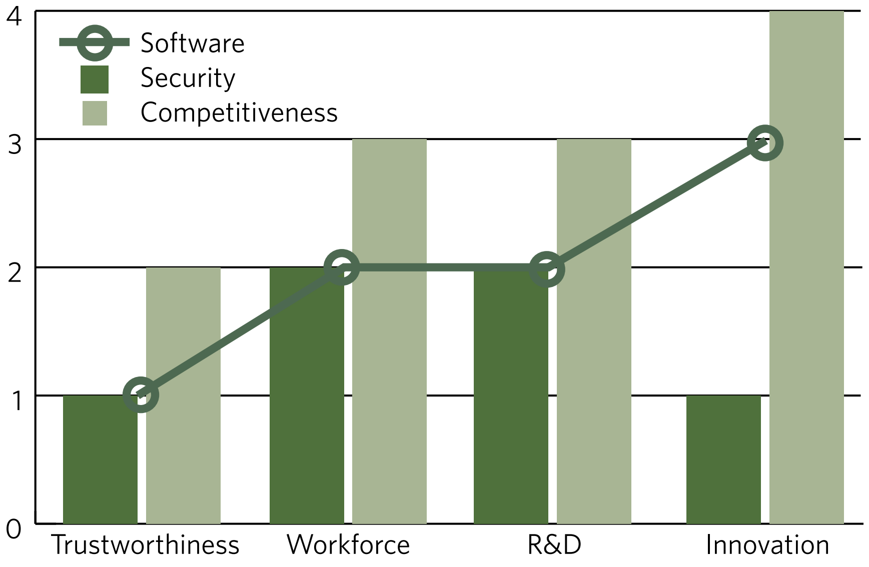
Many issues surround security. Cybersecurity foundations are lacking. Cybersecurity practice is ad hoc and not well understood. Ineffective cybersecurity training and certification programs do not provide an ability to secure large-scale software-intensive systems. Research programs often are misdirected and promise what they cannot deliver. As mentioned above, STEM initiatives cannot deliver the needed results and executives and senior managers are disconnected from the realities they face. Privacy, civil liberties, and concerns about information sharing liability increase resistance and barriers to achieving cybersecurity.

Software

The most valued attribute of software is trustworthiness, and this is achieved through good software engineering and the willingness to manage technical debt. See Figure 3. A trustworthy software system is engineered to rigorously demonstrate completeness, correctness, style, rules of construction, and multiple views in order to be trustworthy, secure and resilient. The body of knowledge for good software engineering spans iterative development, systematic design and programming, rigorous software inspections and software process maturity.

The issues surrounding trustworthiness are deeply rooted. An immature software profession continues to stumble in delivering trustworthy software components, systems, and systems of systems. Delivered software continues to contain weaknesses and vulnerabilities that can be exploited. There is growing software dependence in the nation's critical infrastructure and defense industrial base, both of which depend on assuring trustworthiness. Next-generation strategies and tactics do not build on earlier work, lessons learned and past achievements. Academia is not connected to the needs of entry-level practitioners. The profession of software engineering continues to

Figure 4. National Software Strategy Program Assessment



be stigmatized. Corporations seek to commoditize software engineering and programming by outsourcing them. Not yet managed, technical debt is growing nonlinearly.

National Software Strategy Programs

The state of the National Software Strategy Programs is shown in Table 1 with respect to software, security and competitiveness. These programs focus on improving software trustworthiness, educating and fielding the software workforce, re-energizing software research and development (R&), and encouraging innovation within the U.S. software industry.

In assessing the current state of progress in the National Software Strategy Programs, the following observations are offered. Lack of improvement in software trustworthiness may restrain security but not competitiveness, due to a shortfall in trustworthiness practice and a shortfall in cybersecurity foundations and practice. Limited improvement in educating and fielding the domestic software workforce may restrain security as STEM promise exceeds delivery, but not competitiveness, as this weakness may serve to stimulate offshore outsourcing. Limited software research and development may restrain security with corporate decreases in R&D spending, DoD withdrawal of support for Carnegie Mellon University's Capability Maturity Model Integration (CMMI), and the threat of sequestration looming over the defense industrial base; but competitiveness will not be restrained. Moderate improvement in encouraging innovation within the U.S. software industry may serve to boost competitiveness with "innovation in the small" in evidence, while impacting securitybecause mobile and Bring Your Own Device (BYOD) offer new challenges to cybersecurity. In summary, software practice continues on the one hand to be a challenge revealing itself most evidently as an enabler to the nation's cybersecurity threat; on the other hand, software houses much of the innovation that underlies U.S. global competitiveness. See Figure 4.

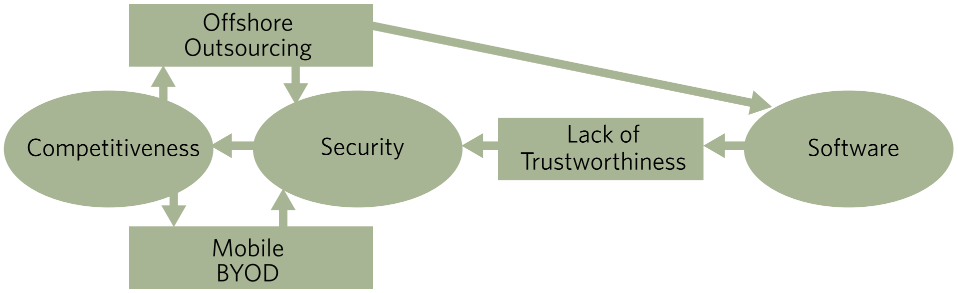
Next-Generation Software Engineering

In accordance with current austerity, the immediate goal of practical next-generation software engineering is to drive systems and software engineering to do more with less ... fast.

Table 1. Status of National Software Strategy Programs

National Software Strategy Programs	Software	Security	Competitiveness
Improving software trustworthiness	• Software trustworthiness foundations known • Shortfall in software trustworthiness practice • Increasing acceptance of technical debt	• Cybersecurity foundations not fully known • Shortfall in cybersecurity practice • Strong focus on software security assurance through Department of Homeland Security/DoD Software Assurance Forums and Working Groups	• Shortfall in software trustworthiness and cybersecurity practice threaten U.S. competitiveness • Strong market in cybersecurity as organizations seek to find perimeter defense and secure in-depth protection
Educating and fielding the software workforce	• Science, Technology, Engineering and Mathematics (STEM) promise exceeds delivery • Domestic software workforce shortfall serves to stimulate offshore outsourcing	• STEM promise exceeds delivery • Shortfall in cybersecurity workforce	• STEM promise exceeds delivery • U.S. competitiveness dependent on offshore outsourcing
Re-energizing software research and development (R&D)	• Corporate decrease in software R&D spending • DoD withdrawal of support for Capability Maturity Model Integration (CMMI) • Sequestration impact looms over defense industrial base	• Continued focus on Critical Infrastructure Protection (CIP) • Inadequate focus on Critical Infrastructure Resilience (CIR)	• Defense industrial base resistance to fixed price contracting
Encouraging innovation within the U.S. software industry	• "Innovation in the small" in evidence • Team innovation management needs improvement	• Defense industrial base focus on CIP not CIR • Mobile and Bring Your Own Device (BYOD) offer new challenges to cybersecurity	• Strong commercial industry product focus on innovation • Defense industrial base examples—i.e., Lockheed Martin Corporation's Innovate for the Future Initiative

Figure 5. Primary Competitiveness, Software, Security Interactions



Four practical objectives are identified to advance this goal using smart, trusted technologies:

- Drive user domain awareness.
- Simplify and produce systems and software using a shortened development life cycle.
- Compose and field trustworthy applications and systems from parts.
- Compose and operate resilient systems of systems from systems.

Wrap-up

Recognize that competitiveness is like floodwater finding or creating its own path. Competitiveness impacts both software and security as it favors offshore outsourcing and further impacts security as innovation drives toward mobile and BYOD. Recognize also that software and security are connected at the hip through the elusive attribute of trustworthiness and together impact competitiveness in a not-so-virtuous cycle of interactions. See Figure 5.

The software situation is dire because we are short on competitiveness, innovation and STEM resources; we are long on offshore outsourcing and technical debt; we are short on trustworthiness and cybersecurity; we are uncommitted to fixed price contracting; and we underutilize next generation software engineering and undervalue the CMMI. The journey no longer has a destination. Fueled by austerity and neglect, trustworthiness, workforce and R&D are in a heightened technical debt. Driven by genuine market forces, innovation and competitiveness are finding their own paths.

If the software industry is to be consequential going forward, it can't just settle for governance and compliance. Instead it needs to be smart and trusted, and it needs to break things ... starting with old habits.

The author can be contacted at **oneilldon@aol.com**.