We are experiencing the fallout from the lunge toward a paperless society without a technology infrastructure. As McNamara said during the Vietnam War, “If you don’t watch the periphery, it will soon become the center” [1]. Security has become the center but a center that spans many dimensions.

Cybersecurity has many dimensions, and currently players are free to choose the dimension that best suits their background, experience, interest, or business objective. The challenge facing the country is to frame the issue realistically, to distill those factors that impact on the national interest, and to do so with intellectual honesty and no self-interest. In large measure, we are engaged in operation barn door, and the horse has already left.

What are the dimensions of security?
• It spans threats, vulnerabilities, and readiness.
• It spans legislative directions with its unintended consequences that impact security.
• It spans the industry’s software products and its inability to field trustworthy software systems.
• It spans industry best practices and certification of processes, people, and products.
• It spans the private and public sector and the tensions between them.
• It spans the industry’s underlying software architecture and environment.

Cybersecurity threats and vulnerabilities are increasing in number and sophistication, but security readiness is hampered by vendors neglectful in product trustworthiness and by an inadequate user commitment to security readiness. Unwise legislation, inadequate public-private collaboration, a patchwork of government regulatory infrastructure, and lack of business incentive completing this inhospitable environment matches shortfalls in technical architecture, product trustworthiness, and security best practices. The debate over who pays for cybersecurity is tilted toward industry and its responsibility to remain competitive, exposing the nation’s critical software infrastructure to predictable security threats. Vendors must make the sacrifices needed to eliminate vulnerabilities; users must invest in resistance, recognition, and reconstitution; and government must communicate, legislate, and regulate to rebalance the business calculation toward security. The community must forge a shared vision spanning realistic assumptions about threats and vulnerabilities and the policy steps needed to achieve survivability.

The following sections discuss these dimensions of security in more detail.

Threats, Vulnerabilities, and Readiness
Security spans threats, vulnerabilities, and readiness. The primary software security focus needs to shift from threats and vulnerability to readiness and survivability. Threats are not well understood. Even as we struggle to determine the profile of future incidents, the analysis of past incidents yields only an incomplete and sometimes contradictory profile. Ninety percent of security threats exploit known flaws, 60 percent are random, and 40 percent are targeted, but the degree of persistence is unknown. While probably 100 percent of U.S. enterprises are attacked, only 30 percent admit to being attacked, perhaps because insiders carry out 70 percent of these attacks. Interestingly, 17 percent of attacks are attributed to industrial espionage and competitive intelligence. What security threats have you experienced?

It is the industry’s software products that make us vulnerable to cyberattack [2]. Current vulnerabilities are predominately in implementation not design. These are examples of neglect and stem from unanticipated input, incorrect usage of protocols and connectivity, and accepting vendor default settings. Understanding these vulnerabilities involves chasing down execution paths and their uncountable large number of possibilities.

Vulnerabilities abound. There were 5,000 vulnerabilities identified in 2001, and approximately 4,000 vulnerabilities in 2002 alone. The same 30,000 hacker Web sites support these vulnerabilities. Also, industry dependence on Microsoft products with its large pool of users and its common and numerous vulnerabilities greatly facilitates security intrusion into the nation’s critical infrastructure, accounting for 90 percent of all vulnerabilities [3].
When it comes to trustworthy software products, Microsoft has forfeited the right to look us in the face. What vulnerabilities are you aware of in actual practice?

Future vulnerabilities may find their way into designs. Security markup language initiatives for common authentication and authorization and those capable of selective word protection in text are innovative. However, these efforts are not validated and there is a lack of research directed at the end-to-end validation of Internet services. Can data streaming through the Internet be tampered with en route, resulting in a security exposure now or later?

If you discover a new vulnerability, what should you do? The reporting of vulnerabilities is in disarray. One vendor has threatened to sue researchers who publicize its security vulnerabilities. The Critical Infrastructure Protection Board advises researchers to contact the vendor before vulnerability is discussed publicly. If the vendor does not respond, the second place to contact is the CERT Coordination Center. Finally, the third place is the Critical Infrastructure Protection Board itself. Clearly a single, independent office should receive all reports and be accountable for analysis, disposition, status, and dissemination of vulnerabilities. These people have invented a strange concept of responsibility.

Regarding readiness, security must be designed in; it cannot be bolted on. Beyond that, there is little consensus on what it means to be ready. Some of the industry approaches to readiness are simply wrong. Some say that security depends on the people doing the protecting, but security cannot be outsourced. Some say security is a journey, not a destination. This brings to mind the saying, “If you don’t have a map, any road will do.” Is it the destination that is unknown or the road to reach it? Many are treating security as a process improvement activity. After 15 years, industry software process improvement has succeeded in stranding 68 percent of its U.S. practitioners at maturity. Levels 1 and 2, below the threshold of competent software engineering, which is Level 3 [4]. Others view security as a risk-management exercise. Hello! We need to be secure now if we are to avoid the digital Pearl Harbor predicted by government officials.

**Architecture and Trustworthiness**

Security spans the industry’s underlying software architecture [5, 6] and environment and its inability to field trustworthy software systems [7]. Industry must make the technical sacrifices needed to achieve enterprise security. Security may require sacrificing certain preferred attributes of trustworthy software systems. For example, openness, interoperability, and modifiability facilitate security intrusions.

In addition, security may require sacrificing certain architectural styles in favor of those that facilitate ease of deterministic recovery and reconstitution following a security intrusion. How many are considering moving from fat clients to thin clients? What technical sacrifices have you made?

**Best Practices and Certification**

Security spans industry best practices and certification of processes, people, and products. The primary software security focus on industry practices and certification must shift from process and people to product. Industry software configuration management practice is poor, and patches are made without adequate testing. Beyond that, the industry practice is to procrastinate on implementing security patches because upgrades lead to problems, and personnel to test and retest are in short supply. What has been your experience? What is the typical frequency of release for your system upgrades?

**Private and Public Sector**

Security spans the private and public sector and the tensions between them. It is necessary to trade knowledge for power in seeking common ground in the public-private collaboration. There is a public and private consensus that industry must take the lead in addressing security. If the private sector does not come up with market-driven security standards, then government will step up its regulatory pace. However, the government itself has earned failing grades on security readiness [8]. In addition, the private sector is reluctant to report security intrusions to the government due to the Freedom of Information Act. Has your enterprise reported any security incidents?

**Legislative Directions**

Security spans legislative directions with their unintended consequences that impact security. It is necessary to revise the legislative actions whose consequences are impacting national security. Unintended consequences have accompanied the Uniform Computer Information Transaction Act, the H1B High Tech Immigration Visa Program, the Clinger-Cohen Act, and the Freedom of Information Act.

The availability of security liability insurance might diminish the incentive to improve the software security infrastructure. Currently insurers lack actuarial data on software security, and may demand compliance with good security practice as a prerequisite to underwriting insurance. Software companies often operate as services and are not subject to product liability. Nevertheless, contractors may be reluctant to support government security initiatives without indemnification from third party liability. Are these topics being discussed in your organization?

**Government Regulatory Infrastructure**

Security spans the government regulatory infrastructure. An enterprise must consider the security cost and information disclosure risk in working with the government. National Security Telecommunications and Information Systems Security Policy No. 11 requires that all commercial off-the-shelf products must be certified by one of several agencies. These are software products that process, store, display, or transmit national security information. It became effective in July 2002.

Presidential Decision Directive (PDD) 63 is intended to promote cooperation between industry and government. The interconnection of the various sectors of the nation’s critical infrastructure introduces the risk of cascading consequences following a terrorist attack whether a physical attack or cyberattack. To counter this threat, Information Sharing and Analysis Centers have been created to gather, analyze, and disseminate information and promote public-private cooperation. However, the Freedom of Information Act is throttling the willingness of industry to participate fully and share openly.
Compliance with PDD 63 is achieved through vulnerability assessments using the Information Security Assessment Training and Rating System administered by several organizations.

The Government Information Security Reform Act requires government agencies to integrate security programs into their computer network and capital investment plans. While the price of noncompliance is a budget cut, heads of government agencies lack the skilled staff to comply.

**Business Incentive**

Security spans business with its lack of an essential driving incentive to promote security. It is necessary to provide effective mechanisms that tilt the essential business calculation from cost effectiveness and competitiveness to trustworthiness, survivability, and security. Enterprise management is driven by quicker, better, cheaper and cost-effective software practices that enhance competitiveness while increasing security risk. Even quality concerns register with enterprise management 10 times higher than security concerns. The high cost of security readiness and the perceived low probability of impact due to security intrusion conspire to promote inaction despite that $13 billion in impact was attributed to security intrusion in 2001. The enterprise must analyze what is to be protected and how important it is to be protected. What needs to be protected in your organization?

The scope of topics under the security tent is broad and deep; consequently, there are no experts. Organizations are now assigning chief security officers to address security in an effort to fence off the blame for this high-risk area. Stovepipe knowledge is increasing with respect to past and current threats and vulnerabilities, but understanding and practicing readiness are lagging. Security threats come from unexpected places. This makes risk management difficult.

The attempt to get a balanced security risk-management program leads to nuanced approaches that look good under the uncrirical light of management review but buckle under the intense glare of the factory floor and operating center. A collection of 90 percent approaches does not yield a 100 percent solution. When there is order, incremental change and process improvement can succeed; but when things are in disarray, the practice of tilting borderline practices towards a center line proves inadequate. The antidote for security threats is survivability. For enterprises with software operations at the center of the nation’s critical infrastructure, nothing else will do.

**Levels of Competitiveness**

The government is responsible for prosperity, and industry is responsible for competitiveness. The leading indicators of prosperity span competitiveness, security, and infrastructure because without security and infrastructure, competitiveness cannot be achieved [9]. The Council on Competitiveness in Washington, D.C., defines competitiveness “as the capacity of a nation’s goods and services to meet the test of international markets while maintaining or boosting the real income of its citizens” [10].

In software, competitiveness is achieved by providing fuel, setting direction, and controlling the environment, including personnel resources, customer satisfaction and added value, competitors and new entrants, and event threats and change [11]. There are five levels of global software competitiveness (see Figure 2):

- **Level 1** is the absence of expectation, achievement, and engagement in the conversation on global software competitiveness.
- **Level 2** is the availability of personnel skills and resources and their deployment.
- **Level 3** is value to the customer derived through vigorous competition for current market niche with mature products that deliver value and earn customer satisfaction.
- **Level 4** is competing for the future by setting the industry standard and practicing reuse and domain architecture technology to meet it.
- **Level 5** is managing change and controlling event threats through strategic software management that raises the ability to improve to a core competence.

**Who Pays the Bill?**

The government has bought in on the security problem, but industry has not yet been sold. Industry appears to treat security as either a business challenge or a business opportunity, but it has not made a commitment to the essential investment of infrastructure. There is a public and private consensus that industry must lead in addressing security; however, with industry slow to take the lead, the government can be heard rattling its regulatory sword in the form of standards.

There is an important national debate on cybersecurity. It centers on who pays the bill, the private or public sector. On one hand, the public sector argues that security and competitiveness move together, therefore, the private sector should pay the cost to be competitive. On the other hand, the private sector argues that security costs too much, and the probability of occurrence is too low to force the investment especially during the period of economic recovery.

**The Trade-Off Factors**

As Deming taught us, there is no substitute for superior knowledge. The knowledge required in this trade-off revolves around the practices and factors that enhance both competitiveness and security and those that enhance one at the expense of the other (see Table 1).

Three types of practices and factors are used to frame the issue, including trustworthiness, cost effectiveness, and survivability. Trustworthiness revolves around an engineering practice that tolerates change and yields dependability of results [7]. Well-engineered software products are complete, correct, consistent, conforming, traceable, simple not complex, scalable, predictable, and usable.
Dependable software products are available, reliable, predictable, tested, defect free, fault free, failure free, stable, private, and safe. Well-engineered software products are also change-tolerant and are adaptable, extensible, interoperable, modifiable, and open.

Cost-effective production is driven by a variety of factors involving personnel resources and skills and development environment and its process, methods, and tools. Specifically, there has been a heavy dependence on several approaches, including using foreign nationals and offshore outsourcing, the incorporation of commercial off-the-shelf products, the deepening of community relations through collaborative research, and the management of personnel factors, in particular personnel turnover.

Survivability spans the resistance to cyberattack, the recognition of a cyberattack, and the reconstitution of enterprise software operations following a cyberthreat or cyberattack [12]. Survivability is achieved through the right blend of function, form, and fit. Function includes user authorization, access control, encryption, firewalls, proxy servers, normal operation monitoring, backup and shadow operations, data and program restoration, and disaster recovery. Form includes dispersion of data, diversification of systems, rules of construction, state data isolation, disciplined data, intrusion usage patterns, virus scans, internal integrity, secure state data monitor, exception handlers, full system state architecture, minimum essential function, and isolation of damage. Fit includes adherence to loading limits, predictable response, no memory leaks, rate monotonic scheduling, timeline or event-driven scheduling, monitor memory management, timeline predictability, watch-dog timer, and full system predictability.

Leading indicators are identified for each practice and form the basis for the trade-off that is structured along the following lines:

- Engineering practices and dependable product factors enhance both competitiveness and security.
- While change tolerance and ease of change benefit competitiveness, they also provide easy access for those with malevolent intent.
- While cost effectiveness benefits competitiveness, some of the means for achieving it present security exposures. Foreign nationals are skilled and cheap [13, 14]; however, they possess the means in the form of superior knowledge and access to intrude on the nation’s critical infrastructure, and they lack allegiance to the United States. Commercial off-the-shelf products provide quick and cheap solutions [15, 16]; however, they are produced with unknown work forces using unknown practices that yield unknown trustworthiness – a security exposure.
- While collaborative research with appropriate intellectual controls is necessary to achieve high maturity in competitiveness, this same knowledge could be used to launch a highly intelligent security intrusion.
- Personnel turnover impacts both competitiveness and security; deep domain knowledge must be kept intramural.
- Survivability practices essential for security impact competitiveness through added cost, product inconvenience, and increased complexity.

The leading indicators (see Figure 3) selected to characterize the practices and factors of competitiveness and security are drawn from the attributes of trustworthy software systems [7], global software competitiveness [17, 18], and cybersecurity survivability [12, 19].

A Web-based scoring and analysis tool is being used to assess the impact of trustworthiness, cost effectiveness, and survivability practices and factors on competitiveness and security. Using this tool, the factor impact analysis was conducted to analyze the behavior of trustworthiness, cost effectiveness, and survivability (see Figure 4). To demonstrate the use of the tool, a set of notional quick-look scores is postulated for commercial, Department of Defense, industry, and government (see Table 2 on Page 28). Participants are asked what scores they would assign each practice and factor and are invited to exercise the tool to complete the analysis [20].

Each practice and factor is rated from low to high on a scale of one to five. The expressions used to evaluate competitiveness and security derives an average of the factors, not weighted. Negative factors shown in Table 1 are adjusted by subtracting the score for the factor from six effectively mapping the one-to-five scale to a five-to-one scale.

The expressions used to evaluate competitiveness and security are:

\[
\text{competitiveness} = \frac{\text{engineering} + \text{dependable} + \text{change} + \text{cost effectiveness} + \text{survivability}}{5}
\]
Survivability

The nation’s software infrastructure is fragile. When it is targeted by a competent, determined attacker, it may collapse. Those who bring their A-game may be able to reconstitute software operations; others will not.

Survivability spans the resistance to cyberattack by improving the software infrastructure, recognizing a cyberattack by sharing information on threats and vulnerabilities, and reconstituting enterprise software operations following a cyberthreat or cyberattack by ensuring continuous operations, switching over, and restarting critical operations. Survivability is achieved through the right blend of function, form, and fit (see Table 3).

The game plan is a software survivability policy that begins by forging a shared vision on the nature of the threat, vulnerabilities, and readiness. This vision assumes that threats continuously evolve, vulnerabilities are large and growing, critical assets are under continuous attack by insiders and outsiders, attacks are targeted and persistent and directed at both system and application, threats and vulnerabilities are outside the control of the enterprise and not fully knowable, and survivability strategies must be independent of threats and vulnerabilities.

The policy establishes a readiness framework for achieving software survivability, one that organizes and orchestrates the layers of security by making an explicit commitment for inaction or action based on security costs exceeding intrusion costs, adopting best security practices in order to avoid lawsuits, performing due diligence in resistance and recognition in order to protect the business enterprise, ensuring the continuous operation of the critical infrastructure through reconstitution, and controlling the disclosure of information to the government and to attackers (see Table 4).

Table 2: Notional Values for Factors

Table 3: Software Survivability Model

Table 4: Software Survivability Policy


Note

1. Dr. W. Edwards Deming is known as the father of the Japanese postwar industrial revival and is regarded by many as the leading quality guru in the United States. He died in 1993.

About the Author

Don O’Neill is an independent consultant who focuses on software inspections training, directing the National Software Quality Experiment, and conducting global software competitiveness assessments. Following a 27-year career with IBM’s Federal Systems Division, O’Neill completed a three-year residency at Carnegie Mellon University’s Software Engineering Institute under IBM’s Technical Academic Career Program. He is a founding member of the Washington D.C. Software Process Improvement Network and the National Software Council and serves as the executive vice president of the Center for National Software Studies. O’Neill is also a collaborator with the Center for Empirically Based Software Engineering.

9305 Kobe Way
Montgomery Village, MD 20886
Phone: (301) 990-0377
E-mail: oneilldon@aol.com