A Theory to Guide US Cyber Security Policy

by Larry Clinton

Former US Central Intelligence Agency (CIA) and National Security Agency (NSA) Director Gen. Michael Hayden noted in his recent article "The Future of Things Cyber" that "rarely has something been so important and so talked about with less clarity and less apparent understanding than this phenomenon."[1]

While there is no shortage of ideas as to how to secure cyber systems, these ideas tend to lack coherence. Cyber security has historically been thought of as an "IT issue." Yet much like the Internet, it is actually an interconnected set of issues with technical, operational, economic, and public policy dimensions. Thought leaders can make a substantial contribution by developing and aligning these interrelated fields in a set of deductive statements that can form the beginnings of a theory of cyber security that can suggest specific policy directions.

This article attempts to start that process by offering seven "syllogisms" of cyber security. While they are not all syllogisms in the classic sense, and the examples are drawn largely from US-based experience, this set of deductive principles does provide a way of thinking about cyber security in a broader context that embraces operational, economic, and public policy dimensions.

SEVEN SYLLOGISMS OF CYBER SECURITY

Syllogism 1

A. If most modern infrastructures rely on cyber systems for their operation,

The US National Infrastructure Protection Plan (NIPP) states:

> The US economy and national security are highly dependent upon global cyber infrastructure. Cyber infrastructure enables all sectors' functions and services, resulting in a highly interconnected and interdependent global network of critical infrastructure and key resources.[2]

B. And if cyber systems are increasingly vulnerable to attack,

> Production of malicious software has reached its highest level, with an average of 60,000 new programs a day.[3]

C. Then most of our critical infrastructures are increasingly open to attack.

There are numerous declarations supporting this principle, among the most recent and stark coming from US CIA Director Leon Panetta:

> The potential for the next Pearl Harbor could very well be a cyber attack. If you have a cyber attack that brings down our power grid system, brings down our financial systems, brings down our government systems, you could paralyze this country. And I think that's a real potential.[4]

Syllogism 2

A. If the government's responsibility is to provide for the common defense,

The US Constitution states that the people of the United States established their government "in order to form a more perfect union,... provide for the common defense, promote the general welfare...."[5]

B. And industry's job is to maximize shareholder value,

This principle (more precisely, to act in the best interests of the corporation) has been well established in US case law going back nearly 100 years.[6,7]

C. Then industry and government, operating from different perspectives, must reach a consensus on appropriate and practical cyber security solutions.

While industry and government have aligned interests, they are not identical. Government is beholden to the general citizenry. In free market economies, industry is beholden to its shareholders. There is synergy between the public sector's and the private sector's goals, but their priorities and roles are structurally different. These differences must be clearly understood and appreciated in order to sustain a productive partnership.

For example, there is broad consensus that the best approach to cyber security is based on risk assessment and risk management. However, the public and private sectors may assess risk differently based on their varying roles and responsibilities.

Industry will primarily use economics to assess risk. For example, if a retailer is aware 10% of its inventory is "walking out the back door" every month, it will increase security — until that costs 11% per month. At that point, the retailer will simply write off the pilfering as a cost of doing business.

Government may not have the luxury of a strict economic assessment of risk. Charged with the higher calling of providing for the common defense and promoting the general welfare, as well as being subject to overtly political considerations rather than simply bottom-line ones, government may well have a lower tolerance for risk than its private sector counterparts.

It may also be the case in an interconnected world that industry may have to move toward government's higher standards in the interest of national security. However, it is also legitimate for industry to expect that it will be compensated for the costs of adopting a standard that is beyond what is justified by its legally mandated commercial responsibilities.

The issue here is not who has the right standards, but rather to recognize that members of a partnership may have legitimately differing perceptions based on their own responsibilities. These differences need to be recognized and accommodated.

Syllogism 3

A. If cyber attacks are increasingly easy, cheap, and profitable to launch,

Just as the Internet is now so user-friendly that even preschool children can use it, cyber attacks have also become far easier to launch. In fact, to become a cyber criminal, one needs virtually no expertise at all. There is now a growing industry that will allow individuals to essentially outsource cyber attacks for a very small investment.

The return on cyber attack investment, on the other hand, can be massive. Estimates as to the amount pilfered vary widely, from the tens of billions[8] to a trillion dollars annually.[9]

B. And if cyber defense is a generation behind the attacker, ROI is difficult to show, and successful prosecution is extremely rare,

Because of the evolving nature of cyber attack methods, it requires continual investment to combat them. Furthermore, a number of factors complicate investment in cyber defense. These range from macro factors, such as the worldwide economic decline, to the fact that traditional investment metrics like net present value and ROI have little value in making security investment decisions, in part because they cannot quantify the benefits that security solutions provide, such as cost avoidance and brand preservation.[10] The result has been that, in many enterprises, investment in cyber security has been deferred or reduced for the past several years.[11]

A further inhibiting factor is that successful prosecution of cyber attackers is exceedingly rare. Most estimates suggest that we successfully prosecute just 1% or 2% of the perpetrators of *all* cyber attacks.[12]

C. Then the incentive structure of cyber security massively favors the attackers.

The conclusion to this syllogism would seem self-evident. So long as attacks are cheap, easy, and profitable, while defense is a generation behind the attackers, problematic to invest in, and rarely yields successful prosecutions, it may not make much difference how good the technology gets. The incentives to attack may be irresistible.

Syllogism 4

A. If most economic incentives favor cyber attackers,

This premise is demonstrated above.

B. And if the costs of poor cyber defense are not directly aligned with penalties for poor defensive behavior,

The problem of interdependent risk occurs when corporate IT infrastructure is connected to other entities in such a way that it leads to failures elsewhere.[13] This risk will lead firms to underinvest in security technology and cyber insurance. For example, assume that a rogue state or criminals attempt to steal intellectual property from a high-value target. Accessing the target directly may be difficult because of substantial investments made to prevent unauthorized entry to its system. However, the same information may be found on less-protected networks belonging to a partner or contractor. Thus, the attack could be mounted against a weaker element in the system.

In such instances, the edge entity on the point of attack may not suffer any economic impact and thus has little incentive to prevent similar attacks. On the other hand, the ultimate target would not only suffer potentially severe impacts, it would also have revealed that its investments are being undermined by an entity on the edge at the point of the attack. Research has confirmed the security downside of such interdependency.

According to Cambridge University's Ross Anderson and Harvard's Tyler Moore:

> Further externalities can be found when we analyze security investment, as protection often depends on the efforts of many principals. Budgets generally depend on the manner in which individuals' investments translate into outcomes, but the impact of security investment often depends not only on the investor's own decisions, but also the decisions of others.... Systems are particularly prone to failure when the person guarding them is not the person who suffers when they fail.[14]

A review of the literature on information security confirms this general finding:

> Economists have long known that liability should be assigned to the part that can best manage risk. Yet everywhere we look we see online risk allocated poorly ... people who connect insecure machines to the Internet do not bear the full consequences of their actions, (and) developers are not compensated for costly efforts to strengthen code.[15]

An unfortunate byproduct of the drive to deploy evermore efficient IT platforms is that efficiency sells far more readily than does security.

C. Then economic incentives must be realigned to create a sustainable system of cyber security.

Again, this conclusion would seem self-evident.

Syllogism 5

A. If 95% of the cyber infrastructure is in private hands,

The exact percentage of privately held cyber systems is subject to differing estimates, but no one contests that the vast majority of cyber systems are owned and operated by the private sector.

B. And if industry is being driven to adopt less-secure technologies and structures to achieve needed market efficiencies,

The recent economic downturn has merely exacerbated industry's need to cut costs to face a global competitive environment. IT, with its history of stimulating productivity while innovating evermore affordable generations of products, is looked to as a major element of enterprise efforts to become more efficient and competitive.

An unfortunate byproduct of the drive to deploy evermore efficient IT platforms is that efficiency sells far more readily than does security, and as a result, newer IT platforms may not be as secure as those they replace.

One other complication arises from the competitive economic pressures that lead enterprises to employ uncertain security measures. For example, deploying unified communications (UC) platforms such as VoIP yield substantial cost savings, but according to the Internet Security Alliance (ISA) report *Navigating Compliance and Security for Unified Communications*:

> While unified communications offer a compelling business case, the strength of UC solutions in leveraging the Internet to transform how we communicate is also a vulnerability. Not only are UC solutions exposed to security vulnerabilities and risks that the Internet presents for other corporate network activity, but the availability (and relative youth) of UC solutions has encouraged malicious actors to develop and launch new types of attacks.[16]

A similar example involves cloud computing. Just like VoIP, cloud computing has emerged as one of the hottest developments in IT, largely driven by such perceived economic benefits as cost savings and efficiencies.[17] And as with the VoIP deployment, security may be undermined because of competitive pressures driving cost reductions. A recent survey found 62% of respondents acknowledged having little or no faith in the security of the data in the cloud, including 49% who had already placed their data in the cloud![18]

In addition, business strategies that optimize customer intimacy and supply chains require companies to connect to vendor and customer networks. While tighter integration with business partners provides clear business benefits, it also means the ability to defend against attacks depends on your partners' or customers' security capabilities and policies.

C. Then an effective cyber security policy will need to lower cost or increase rewards for private sector cyber security investment.

It has been noted above that industry's legal mandate is to maximize shareholder value and that investment in cyber security in many enterprises is being deferred or reduced despite the growing cyber threat. It should come as no surprise that the main reason for this constrained investment is cost.[19]

Yet public policy has to date largely ignored this fundamental set of facts. For example, while numerous bills to address cyber security have been introduced in the

US Congress, none of these measures, nor programs being implemented by the Obama administration, are designed to assist enterprises in enhancing their security by reducing or compensating for the increased cost. Instead, most proposals to improve cyber security lay out new prescriptions that industry will be directed to follow and the costs of which it will presumably be asked to absorb.

Syllogism 6

A. If infrastructure enhancement is historically promoted via market incentives,

Roughly a century ago, an analogous set of circumstances arose in the US when policy makers concluded that the new technology infrastructures of the time — telephones and electricity delivery — were not adequately serving the general public interest.

Government understood that the general welfare would be best served not by taking over these infrastructures, but by working with the private sector on the twin goals of continually enhancing the infrastructures and also ensuring that there was universal service to the populace.

The result was that government and industry struck a social contract, wherein government facilitated private investment in these critical infrastructures by guaranteeing the rate of return on private investments in the infrastructure, while industry took on the burden of providing universal service, which would have been otherwise uneconomic. These companies then became known as privately owned public utilities. This social contract was implemented usually through the creation of public utility commissions at the state level.

B. And if regulation is not an effective mechanism to create sustained cyber security,

Cyber security is a unique issue area that may be especially difficult to address by using the traditional federal regulatory structure. No less an authority than President Obama — rated one of the most pro-regulation members of the US Senate during his tenure there[20] — has observed that the interconnected nature of the Internet makes using regulations to secure it highly problematic[21] and has pledged not to follow that course.[22]

Moreover, even if government could create an effective set of regulatory mandates or impose liability on vendors for insecure systems, it would likely face protracted litigation; the technology changes so quickly that keeping the standards current would be a daunting task. There is also no assurance that government regulations would be effective. Given the inherently political nature of the regulatory system, it is at least as plausible that the regulations that emerged would be watered down, much as US campaign finance regulations are.

There is also the very real possibility that government mandates could turn out to be counterproductive. There is some evidence that current security mandates may actually be leading to lower security, as organizations redirect the personnel and time formerly devoted to security activities to regulatory compliance instead.[23] One major multistate company recently told me that they had gone from quarterly penetration (a best practice the ISA endorses) to annual testing because they were too busy with largely redundant audit compliance. That's a 75% reduction in one of the most effective practices in the field due to resources being diverted to compliance. It seems that many firms now fear the auditor more than the attacker.

In a larger context, even if a set of regulatory mandates could work, they would have to be balanced with the negative effects they could have on innovation, investment, and industry cost. While some industry is inherently tied geographically to the US, many industries — including defense, IT, and manufacturing — could become motivated to move their operations to less-regulated locations.

It seems that many firms now fear the auditor more than the attacker.

C. Then a cyber security social contract using market incentives will be a comparatively more effective mechanism to stimulate investment in cyber security.

It has been argued in greater depth elsewhere[24, 25] that we face a problem with cyber security similar to the one we faced a century ago with telephone and electric systems. In both cases, we have enormously promising innovative technologies that we curb at great risk. On the other hand, we have significant social issues that must be addressed by enhancing the infrastructure. Just as a century ago, we needed to completely rethink the roles of government and industry in light of massive technological innovation; today's cyber systems demand the same degree of innovation. Twentieth-century regulatory models are unlikely to be suitable

for 21st-century technological issues, including security. A new social contract must evolve that redirects the economic incentives so a sustainable system of cyber security can arise.

Syllogism 7

A. If private sector investment decisions are made on a company-by-company basis,

Government sometimes seems to believe that the private sector is a unified entity. In reality, the "private sector" is only a collective noun representing millions of independent entities.

As a result, the investment decisions regarding upgrading cyber security must be relevant and powerful enough to attract the decision makers in these corporate boardrooms and offices.

To be effective, market incentives must speak to the private sector at the business plan level.

B. And if companies have varying business plans, regulatory environments, cultures, and structures,

Even fairly cohesive industry sectors, such as electricity generation or chemical production, have individualized company business plans and cultures. The differences become even more dramatic when we consider less-regulated critical sectors such as IT and defense. When we compare various sectors, the differences between them in terms of what is relevant to their investment decisions can grow even larger.

To be effective, market incentives must speak to the private sector at the business plan level. An R&D tax credit may be the most attractive option for an IT security vendor, while a defense firm may be more interested in procurement options, an electric utility in a streamlined regulatory environment, or an IT-user enterprise in an insurance discount and risk transfer.

C. Then government and industry need to offer a menu of market incentives that will induce organizations with varying business plans to deploy adequate cyber security.

In March 2011, an unprecedented group of US industry associations and civil liberties interests released a comprehensive white paper on cyber security that articulates a specific path toward a more secure system. The paper, which tracks the organization and issues raised in President Obama's *Cyberspace Policy Review* (*CSPR*), is remarkable as much for the detail of its recommendations as the breadth of its authorship, which includes organizations empowered by their thousands of corporate members to represent the interests of users, providers, and the owners and operators of the Internet.

The paper states:

> One of the most immediate, pragmatic, and effective steps that the government could take to improve [the US's] cyber security would be to implement the recommendations made in the *CSPR* to explore incentives, such as liability considerations, indemnification, and tax incentives …

Specifically, it recommends:

> Working through the NIPP framework, government and industry must develop a menu of market incentives that government can put in place to motivate companies to voluntarily adopt additional security practices and technology investments. The incentives must be powerful enough to affect behavior without being so burdensome as to curtail US investment, innovation, and job creation.[26]

Up to now, the emerging field of cyber security has been construed too narrowly as an IT issue. A more robust analysis of the field would be facilitated by developing a set of logical principles that interconnect economic, strategic, and technical issues of cyber security. In this article, I have offered seven such syllogisms, which suggest that government and industry need to engage in a 21st-century social contract to create a sustainable system of cyber security.

ENDNOTES

[1]Hayden, Gen. Michael V. "The Future of Things Cyber." *Strategic Studies Quarterly*, Vol. 5, No. 1, Spring 2011.

[2]*National Infrastructure Protection Plan*. US Department of Homeland Security (DHS), 2006.

[3]Clapper, James R., Director of National Intelligence. Testimony before the US Senate Select Committee on Intelligence, 112th Congress, 16 February 2011.

[4]Panetta, Leon, CIA Director. Testimony before the US House Permanent Select Committee on Intelligence, 112th Congress, 11 February 2011.

[5]US Constitution, preamble.

[6]*Dodge v. Ford Motor Co.*, 204 Mich. 459, 170 N.W. 668. (Mich. 1919)

[7]*Carlton Investments v. TLC Beatrice International Holdings, Inc.* No. 13950 Court of Chancery of the State of Delaware, New Castle, 30 May 1997.

[8]Lewis, James A. *Cybersecurity Two Years Later*. Center for Strategic and International Studies (CSIS), January 2011.

[9]*Unsecured Economies: Protecting Vital Information*. McAfee, Inc., 2009.

[10]"How IT Is Managing New Demands: McKinsey Global Survey Results." *McKinsey Quarterly*, November 2010.

[11]*The Financial Impact of Cyber Risk: An Implementation Framework for CFOs*. American National Standards Institute (ANSI) and Internet Security Alliance (ISA), 2010.

[12]Regoli, Robert M., and John D. Hewitt. *Exploring Criminal Justice: The Essentials*. Jones & Bartlett Publishers, 2010.

[13]*The Internet Security Alliance Answer to the Department of Commerce Notice of Inquiry: Cybersecurity, Innovation and the Internet Economy*. ISA, 20 September 2010.

[14]Anderson, Ross, and Tyler Moore. "The Economics of Information Security." *Science*, Vol. 314, No. 5799, 27 October 2006.

[15]Anderson and Moore. See 14.

[16]Waters Edge Consulting, LLC. *Navigating Compliance and Security for Unified Communication*. ISA, 2009.

[17]Yoo, Christopher S. *Cloud Computing: Architectural and Policy Implications*. Technology Policy Institute, January 2011.

[18]"Global State of Information Security." *CIO*, 15 October 2010.

[19]Baker, Stewart, Shaun Waterman, and George Ivanov. *In the Crossfire: Critical Infrastructure in the Age of Cyber War*. McAfee, January 2010.

[20]Friel, Brian, Richard E. Cohen, and Kirk Victor. "Obama: Most Liberal Senator in 2007." *National Journal*, 31 January 2008.

[21]*Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. The White House, Executive Office of the President, May 2009.

[22]"Remarks by the President on Securing our Nation's Cyber Infrastructure." The White House, Executive Office of the President, 29 May 2009 (www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure).

[23]Corman, Joshua. "Rugged Software: Educate IT and Business Professionals to Improve Software Quality and Security." Presentation to the *US Department of Homeland Security Software Assurance Forum*, McLean, Virginia, USA, March 2010.

[24]*The Cyber Security Social Contract: 2.0*. ISA, December 2009.

[25]*The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and 111th Congress*. ISA, 2008.

[26]Business Software Alliance, Center for Democracy & Technology, US Chamber of Commerce, ISA, and TechAmerica. *Improving Our Nation's Cybersecurity through the Public-Private Partnership: A White Paper*. ISA, 8 March 2011.

Larry Clinton is President and CEO of the Internet Security Alliance (ISA). ISA represents major corporations from the aviation, banking, communications, defense, education, financial services, insurance, manufacturing, technology, and security industries. ISA's mission is to integrate advanced technology with economics and public policy to create a sustainable system of cyber security.

Mr. Clinton is one of the clearest voices on cyber security. He has been featured in mass media such as USA Today, *PBS News Hour, CBS Morning Show, Fox News, CNN, C-SPAN, and CNBC. Mr. Clinton has authored numerous professional journal articles on cyber security and has served as guest editor of* Cutter IT Journal. *He is regularly called upon to testify before both the US House and Senate. In 2008, ISA published its* Cyber Security Social Contract, *which is both the first and last source cited in the Executive Summary of President Obama's* Cyberspace Policy Review, *which also cited more than a dozen ISA white papers — far more than any other source. Mr. Clinton can be reached at lclinton@isalliance.org.*