WHITE PAPER.

Understanding the National Strategy to Secure Cyberspace: Mandate or market force, does the motive really matter?

By Ed Hogan, Director, Defense & Domestic Security Programs, Global Public Sector

Even the title sounds ominous—***The National Strategy to Secure Cyberspace***, ugh! Although the 70-plus-page document may not be relaxing bedtime reading, an understanding of its intent is vital to securing business-critical information infrastructure.

Heard of it, but not sure what it's all about? The Strategy outlines an "initial framework for both organizing and prioritizing efforts." Basically, it's meant to educate, increase awareness and motivate action—to put cyber security center stage. While more than half the message is about raising awareness, it's meant to inculcate industry with the need for action and to make non-governmental entities cheerleaders, advocates and apostles of buttoning up the gaping holes in cyberspace.

The final release.

The Strategy outlines the steps that industry, government and citizens need to make to increase the protection level of our nation's cyber infrastructure. While some say it's less a strategy and more a list of best practices, there is strong emphasis on the public-private partner-ship—where cooperation and information sharing between government and the private sector is critical to ensuring the successful implementation of the Strategy.

Although an important step in the right direction, critics have called it disappointing and toothless because it lacks regulatory mandate. What the Strategy lacks in requirements, it makes up in argument for security—with the Internet at the core of the case for vulnerability. Of primary concern is the potential for debilitating disruption to critical commercial sectors, economic well being and, of course, national security.

Despite critics and the document's size, like it or not, it will be existing market forces that pressure industry into tackling cyber security. Market forces, which unfortunately now include computer viruses and cyber terrorists, provide more motivation than government could hope to mandate. Regrettably, it isn't just a scare tactic anymore.

Appreciating threats and vulnerabilities.

Stated objectives of the Strategy are to prevent cyber attack, reduce vulnerability and minimize damage and recovery time – noble causes all. In reality, the growing interdependency and uncertainty in business today is enough to facilitate action given an understanding of the issue. Although almost every organization has experienced some level of cyber intrusion, in most cases how well a company plans dictates how well it reacts and how much remediation ultimately costs. In understanding the threat, the business case makes itself.

Take as example any business, large or small. Ask "what's the potential for disruption and debilitating cost, if your order entry system shuts down for several days? How would you recover information or repair damage? What's the potential lost revenue should your infrastructure collapse due to virus attack? What if you housed critical customer data, private data, in a hacked database? How would customers react?"

Understanding vulnerability is only a part of the picture, there's also uncertainty about potential threats. Cyber attack can come from anywhere, disgruntled internal threats, external predators or global fanatics. Increasing interdependency and uncertainty will soon be enough to make sure those with whom you conduct business are secure partners, secure suppliers, secure customers.

To incite action beyond just understanding, the National Strategy lays out the Five Priorities for Cyberspace Security—here's how your business can participate, prepare and plan to minimize the risks of cyber threat.

We want you!

According to the White House, the Strategy was developed to "engage and empower Americans to secure the portions of cyberspace they own, operate, control, and with which they interact." Simply put, unlike physical space everyone is responsible for cyberspace. It brings to mind the pointing finger of an Uncle Sam poster. This means you—industry and individual, corporation and citizen, public sector and private.

Still, the Strategy strongly puts the onus on private industry. The role of government is not the strong overseer some had hoped for, but the conciliatory coordinator. "The Federal government's role is justified only where the benefits of intervention outweigh the associated costs," the Strategy pronounces.

Does that mean industry bears the weight of securing cyberspace? Frankly, yes, for the private sector "owns" 90% of the nation's cyber infrastructure. Thus, the private sector is better equipped to respond and quicker to react given the speed of most attacks. In large part, that's the way it has to work—the way it will work best. Just ask yourself if your company can afford not to take action, to wait for the government to do it for you. Then decide how you'd like to transfer your next file.

Sharing data—mine, yours, ours.

Relying on infrastructure to share data, files and documents among different physical, geographical and logical systems is just one of the forces increasing cyber vulnerability. Moving information not only between applications, but across boundaries of systems and networks has blurred the lines and created new spaces where ownership is blurred as well. Take for example data exchange in cyberspace—companies share data with suppliers, employers share data with benefits providers, banks share with financial partners, insurers with hospitals, utilities with regulators, ad infinitum.

Who polices the data during exchange? You wouldn't trust just anyone to deliver important documents to the post office or cash to a bank. Why do the same with information?

Determine if you trust partners enough to interact with them. Can you require those you do business with, partners, suppliers and customers, to embrace procedures and technology that decrease their threats and in turn your vulnerability? Soon your cyber security profile may be required as authorization to interact just as VeriSign certifications are the norm at Web retailers. An organization's own best interests are at stake in adopting security. It's not just smart business, it's becoming a business requirement.

Crack one, hack all.

Why is the government asking for volunteers? The government correctly recognized it couldn't regulate the solution. From the beginning a mandate was undesirable, because it's impossible to legislate criteria affecting everyone from corporations to home users. It's too broad a space to dictate and to mandate would mean bowing to the lowest common denominator—an approach that most likely would impede technological progress and erode system performance, as well as require undue spending.

Business can't step back in this e-commerce world, needs differ, environments differ, solutions differ. While each entity has its own agenda, dependencies are increasing, reliance on interconnected systems continues and the number of touch-points inside and outside your company, your industry and your geography grow exponentially in this globally interconnected society.

Common criteria would result in a less flexible, less secure solution. Responses dictated by government would be more homogeneous, having similar architectures set against a common set of requirements. If you're a hacker, that makes things easy—crack one and hack them all.

Success or failure—it depends.

Although it couldn't come at a worst time in terms of the downturn in the economy, the war with Iraq or the government's fiscal budget crisis, the call to action is really a call for investment. It is a call meant to motivate, company by company, industry by industry, to make the investment. Though aside from being costly, how the Strategy will be judged is an outstanding question. Security has always been about risk reduction and since nothing can ever be made 100% secure the real question is can the Strategy help minimize risk.

This time next year, answers to a few key questions may predict success or failure, at least in terms of the Strategy's impact on industry. How long can you wait to answer to these questions:

- What do you know about your own vulnerabilities?
- Have you minimized the impact of known threats?
- How prepared are you should something happen?
- How well are you able to handle intrusions or attacks when they do occur?
- Have you been able to mitigate the impact as much as possible?
- What is the cost of continuing business as you know it?

What happens next is anybody's bet. With continuously evolving threats, advancing technology and the race to stay ahead, we will never be able to eliminate the threat entirely, but we can take steps to manage the risks.

Whether you wait for government policy to dictate or act preventively—you still have to understand cyber security, embrace it and take action.

Beyond just understanding: National cyber security priorities & planning.

"Securing cyberspace is a difficult strategic challenge that requires coordinated and focused efforts from our entire society…." According to the National Strategy to Secure Cyberspace, the recommendation is to take actions consistent with the Strategy. Exactly what does that mean?

Communicate and collaborate. Essentially, it boils down to five points that focus on communicating better to improve awareness and response to cyber incidents, and collaborating to reduce the potential impact from cyber attack. The five priorities outlined cover specific recommendations about:

1) Response systems: analysis, warnings, coordinated views and response, contingency planning and crisis management

2) Threats and vulnerabilities: assessment and consequences, physical and logical interdependencies, mechanisms for trusted computing, securing the Internet and assessing emerging systems
3) Awareness and training: training, education and awareness, and professional certifications
4) Government systems: securing Federal cyberspace
5) National and International legalities: cyber crime, counterintelligence, tracking and attribution, U.S. security, international protection and warning/watch networks

The Strategy recommends a combined role of public-private engagement to facilitate collaboration on at least the first three of the five priorities. (Priorities 4 & 5 are deeply imbedded in the public sector.)

One of the benefits of a non-regulatory strategy is that industry gets to react in a collaborative way, rather than having an edict of must do. It's in industry's best interest to be proactive and innovative, rather than spend time, money and effort in conforming. The question is where to start?

Public/private partnership.

While the public/private partnership will take on a variety of forms and issues, the first step is raising awareness—meaning analysis, watch and warning activities, information exchange and restoration efforts. The remaining recommendations include training, improving technology, stimulating market forces, identifying and remediating vulnerabilities, exchanging information and planning recovery operations.

In applying training and technology, it's important to appreciate the differences between capital investment and investing in human capital, using people resource and effectively upgrading through awareness and training. The best technology solutions are worthless unless your people or those you count on to run your business processes are both aware and smart.

If using good people is half of the equation, the other half is pioneering new technology. Here again, market factors will stimulate technology suppliers to invest in creativity and innovation to meet the need. Individual firms will be forced to invest in technology to remain viable, competitive and to limit liabilities. In this healthy competitive environment, cyber solutions will advance to close the gap much like biometrics and other integrated intelligence tools are already doing. Supply and demand will drive better solutions than government could mandate.

In addition to collaborating, exchanging information is essential to identifying and remediating vulnerabilities. Alerts and notices, knowing something is happening and responding as rapidly as possible, is critical to shorten the time between knowing and acting. In planning recovery operations, best practices and experience play an important role in business contingency and continuity planning. Yet, the key word in planning recovery operations is PLANNING. It can make the difference between reacting and recovering.

Zero-Gap Planning.

Any good plan starts with analysis and assessment. A vulnerability assessment that thoroughly analyzes your risks, business needs, vulnerabilities and threats, and gauges the impact of potential disruption and damage is critical to good planning. And, key to assessing the potential risk are knowledge, expertise and experience in assessing cyber threats. That's where external resources like Unisys bring more than just value.

If yours is a business model where security skills are not considered a core competency, asking your internal security staff to focus on cyber security is probably not an option. Working with a security expert with a proven process for analyzing business needs against the cyber security environment will undoubtedly speed your ability to react and recover from the next virus or attack.

Unisys has the technology and service expertise to help protect business infrastructure and protect the information that keeps businesses in business. Unisys secures organizations from top to bottom using a unique approach called Zero-Gap Security Planning. It helps identify the gaps in security plans, measures and procedures, and supports overall business goals while integrating all levels of the organization for a comprehensive protection plan.

While no solution is 100% guaranteed, in Zero-Gap Planning security teams work to develop a fortified cyber defense landscape, capitalizing on expertise in a variety of critical industries. Security services are guided by Unisys Security Architecture, a holistic approach that marshals solutions and services enabling customers to build a multi-layered security infrastructure for e-commerce in transaction-intensive network infrastructures as well as single network domains.

In addition to providing technology and process solutions, external experts can monitor and manage your cyber security on an ongoing basis. With a full set of security solutions, outside security experts can do more than protect your network, they can protect your entire business by helping you manage risk and minimize vulnerabilities across the entire enterprise.

A role for your company.

In addition to securing your own cyberspace, the government has another role for business. The Strategy outlines the expected role of the private sector in what's referred to as the public/private partnership. It also provides a full catalog of critical commercial infrastructure sectors, which lists just about everyone, including banking and finance, insurance, chemical, electric, oil and natural gas, water, information and telecommunications and transportation. That doesn't mean that those not included get a pass. Accordingly, it's the responsibility of each company, regardless of industry, to have an active security policy, audit programs and instill best practices, as well as facilitate communications.

Yet, it's much more effective if individual companies approach cyber security as a part of an industry—to educate and lobby others to have an equal approach. The Strategy recommends the creation of Informed Sharing and Analysis Centers (ISACs) to monitor and direct respective industry infrastructures in the event of a cyber attack. ISACs are meant to share institutions and mechanisms across industry sectors, reduce risk by developing best practices, evaluate technology advances and certify new technology products.

The greatest benefit of the ISAC is in information exchange—sharing information about attacks, trends, vulnerabilities and best practices. By being involved the individual company is more current on requirements, issues and solutions relevant to the particular industry. More importantly, it provides a forum for not having to address the issue alone. One company doing a superb job does not solve the problem.

The goal should be making the overall business and specific industries better equipped to prevent, reduce and mitigate the impact of cyber attack. In reality, market forces again come to bear. While collective measures are noble, those who actively embrace the challenge and create a plan are much better equipped to handle the inevitable, much quicker to respond and recover, much better able to minimize effect and cost. In the long run, these are companies that will be recipients of a formidable competitive advantage.

Ed Hogan: Bio.

Edward Hogan is the Director of Defense and Domestic Security Programs at Unisys, where he is responsible for coordinating and leveraging the entire company's capabilities and solutions relevant to meeting market requirements to insure security of citizens, business and government. He works with all segments of the company to bring Unisys services and solutions to defense agencies and military services worldwide.

Ed is a Unisys employee of more than 30 years with additional valuable experience in government. Prior to his current position, he served as vice president, Marketing and Strategy for the Global Public Sector industry group. In that capacity, he directed the full range of marketing functions of Unisys Global Public Sector entities worldwide including strategy development, alliances and government relations. Ed also served as vice president of market development and planning for Unisys Federal Government Group, where he managed strategic marketing, marketing support, strategic planning, and market research in the U.S. Federal Government environment.

Ed is a retired U.S. Navy Commander with over 25 years of active and reserve service. He served as a petty officer on destroyers in the North Atlantic. Following university, he was commissioned and was an information technology officer on the staffs of both the Chief of Naval Operations and the Joint Chiefs of Staff at the Pentagon on activities related to command and control and crisis management. Prior to his retirement he was a staff officer for politico-military plans and policy, Office of the Chief of Naval Operations.

He holds a Bachelor of Science in Business Administration from Clark University in Worcester, Massachusetts. Ed and his family reside in Middleburg, Virginia.

Printed in U.S. America