ESAAG
THE KEY TO SECURITY AND AVAILABILITY

The National Strategy to Secure Cyberspace: What It Means To the Large Enterprise

A White Paper of ESAAG, LLC

Version 1.4

Date: September 30, 2002

Enterprise Security and Availability Group, LLC (ESAAG)
3055 Treat Blvd. #37
Concord Ca. 94518
(925) 766-5876

ESAAG White Paper

Table of Contents

Executive Summary

"*The National Strategy to Secure Cyberspace*" is not the information security panacea that was hoped for by those executives responsible for information security in large enterprises. It provides suggestions but there are no "teeth" to it, there are however some good strategic pointers you need to be aware of. Part of the post-9/11 US national security effort, the strategy was released by the President's Critical Infrastructure Protection Board in draft form September 18, 2002. It reflects awareness that the Internet has become a foundation for conducting business, for government operations, and even national defense. The strategy also reflects that the Internet is at risk from an increasing level and variety of threats and vulnerabilities. For this purpose, the strategy identifies 24 strategic goals and 85 recommendations to develop a capability to better manage the threats and vulnerabilities of cyberspace. These were directed to all sectors of cyberspace users and both the public and private owners of cyberspace infrastructure. Of these, three goals and seven recommendations are specific to the large enterprise.

The strategic goals have the common premises that protection of the whole is obtained by empowering each to secure their own portion of cyberspace and that security efforts must evolve as fast as or faster than new threats. The seven strategy recommendations when summarized suggest that large enterprises should

1. take ownership of the security problem at the highest executive levels,
2. adopt basic security best practices, and
3. enter into a partnership to share information with government agencies.

Unfortunately, the only empowerment the large enterprise will realize is an unsuccessful attempt to increase the level of pressure on senior executives to "own" the security problem. To accomplish this, there are five specific questions (in the following box) that boards, investors and analysts should now ask concerning how their organization is addressing security.

Questions corporate boards, financial analysts and investors should ask:

1. What board members are responsible for IT security and risk management oversight? Do these members provide an annual report to the board?

2. Who is the senior most corporate official responsible for IT security and to whom is he or she directly accountable?

3. How often do the CEO and COO review IT security and the overall corporate risk management?

4. What internal IT security policies exist and do they involve annual training of all employees?

5. Are the security controls of the companies computer systems sufficient to prevent unauthorized access to files, alterations of data, loss or theft of trade secretes and assets?

The enterprise needs to understand the answers to these five questions, but they do not raise new issues and do not change the formula about who owns the security problem. Likewise, the seven recommendations bring nothing new to the enterprise. One recommendation, to share information with government agencies, is still not a good idea. There still are no protections in place that allow the agencies to protect what you tell them. All of the other recommendations should be considered best practices. At least the document is asking the enterprise to begin to think about the security problem in strategic terms, not tactical.

The discerning enterprise executive would likely admit that the specified strategy goals and recommendations are probably the right things to do. After all, the tremendous savings possible from use of cyberspace for business are hampered by lack of trust in those systems. It is also much cheaper to prevent attacks than clean up after they are over (assuming you even survive them). However, it is likely not clear which of many efforts should get priority. To this end, ESAAG presents ten steps below that will enable the large enterprise to leverage the "new executive ownership" the strategy brings forward and to help your organization filter down to the parts of the security issue that are most important to you and integrate them into your existing enterprise strategy.

1. Develop or revisit your enterprise security strategy to addresses threat management.
2. Become active in the public and industry-specific debates about security.
3. Educate yourselves and your enterprise about what your threats and vulnerabilities really are.
4. Start thinking in terms of creating ongoing proactive security processes.
5. Think beyond managing only known threats.
6. Buy smart. Factor in security as a requirement and a cost. Look at the true ROI!
7. Establish an Incident Response Team.
8. Think global in scale. The defined network perimeter does not exist any more.
9. Don't use the "National Strategy to Secure Cyberspace" as a model for the enterprise.
10. Don't wait for new international standards to guide your enterprise security strategy.

Introduction

The following white paper is a discussion of what the "*The National Strategy to Secure Cyberspace*" draft means for the large enterprise. The discussion is not intended to support or refute the strategy, but point out the issues that may deserve special consideration as a large enterprise begins the process of assimilating the national strategy into their own strategy. *(A full copy of the strategy document can be obtained at: www.securecyberspace.org.)* The discussion covers where we are now, what we can do next, and where the return is for this investment. A summary of what the strategy asks of us is in Appendix A, for those who have not yet read the strategy document or want a refresher.

Where We Are Now

"*The National Strategy to Secure Cyberspace*" was released in draft form September 18, 2002. Produced by the President's Critical Infrastructure Protection Board, the expressed intent is to provide a roadmap that will coordinate efforts to secure cyberspace. This document, together with Executive Order 13231, captures the statement of United States national policy for emergency preparedness and the protection of critical infrastructure from natural and intentional acts. It is part of the post-9/11 national security effort. The document also brings new focus to existing governmental agencies' efforts, defines an expanded government collaboration with the private sector that actually owns and operates 85% of cyberspace, and is intended to serve as a model for the private sector for how each should plan the protection of it's component pieces. The strategy is strictly voluntary which means that companies may or may not choose to comply with the recommendations. Most security experts feel the document presented the same recommendations we have been making for years, but still does not contain a mandate to implement them.

The document reflects awareness that the Internet has become a foundation for conducting business, for government operations, and even national defense. Although many businesses have adopted use of the Internet with varying degrees of enthusiasm, by July, 2002, the Internet has over 160 million host computers. This shift has resulted in great increases in efficiency and productivity but it has become a dependency that has not come without large costs. Cyber attacks to and over the Internet have impacted these users, costing billions of dollars, significant enough to impact the national and the world economy. Because attacks have doubled over the last year and are projected to increase 400% over the next 4 years, business, government, and critical national services are increasingly at risk.

A small number of the cyberspace threats and vulnerabilities are new types; most threats or vulnerabilities (or variations of them) have been with us a while. For example, rapidly evolving or new technologies, like wireless networking, do not emerge any more secure than their

predecessors. Fortunately, most of these security problems, old and new, can be solved simply by following good security practices, but the cyberspace community has so far failed to implement and follow them. Likewise there have been previous national initiatives to secure cyberspace (Presidential Decision Directive 63, 1998) that have not resulted in significant improvements.

The increasing dependency on cyberspace that runs on an infrastructure which is vulnerable to an increasing level of attacks, presents an unprecedented threat that calls for an unprecedented coordination to secure it. So far, large enterprises have not done very well to secure cyberspace and the trend is getting worse. Unfortunately security is still looked at by most organizations "as a burden to doing business", instead we should be looking at security as a tool that will help the organization meet their goals.

"*The National Strategy to Secure Cyberspace*" is focused on the United States but the task of securing cyberspace must transcend governments, national boundaries, and individual businesses. Cyberspace is a global resource that transcends geography and it will require a global effort to secure it. International enterprises have the most to gain from use of cyberspace and are uniquely positioned to do the most about security of cyberspace.

What the Strategy Asks of Large Enterprise Businesses

The strategy document presents seven specific recommendations for the large enterprise (see Appendix B). The seven recommendations are basic security 101 recommendations, the same issues we should already all be aware of, and are totally voluntary. There are no plans to regulate or require enterprises to make any changes, not even for sectors that own and operate critical infrastructure. For enterprises in a critical sector that are otherwise already regulated, the previously designated lead government agencies for each of the critical infrastructure sectors are unchanged (some changes to Homeland Security are proposed but pending). For all other enterprises, the onus is still clearly on the enterprise to each take care of themselves, which will add to the security of the whole. However, the Administration is now reserving the option to propose new regulation if there is inadequate industry response to the recommendations.

The operative words used are "encourage", "empower", and "foster responsibility". For the large enterprise, this includes 5 questions that corporate boards, financial analysts and investors should ask. These questions attempt to position responsibility for cybersecurity within the enterprise as a senior executive fiduciary duty. The senior executive is responsible to start the process of getting security best practices in use. This is nothing new to most enterprise executives but it may bring higher awareness of security issues to corporate board members and

shareholders, hopefully forcing senior executives to now address these issues - it should be defined as part of their job. The recommendations are not so much a roadmap for how the large enterprise is to achieve security, as a statement of how the government and the rest of the world has changed and will thereby oblige the enterprise to change the way it does business.

1. What board members are responsible for IT security and risk management oversight? Do these members provide an annual report to the board?
2. Who is the senior most corporate official responsible for IT security and to whom is he or she
3. How often do the CEO and COO review IT security and the overall corporate risk management?
4. What internal IT security policies exist and do they involve annual training of all employees?
5. Are the security controls of the companies computer systems sufficient to prevent unauthorized

For companies that are in a business sector with critical infrastructure, the stakes are higher. If your enterprise sector is in banking & finance, electric, oil & natural gas, water, transportation (rail), information & communications, or chemicals, your company is part of the critical infrastructure and your security issues are considered a matter of national security. The regulatory framework for your company is already in place. You are likely already a member of an industry association devoted to security issues and you are paired with at least one Federal agency that is tasked with your support. Each sector also has an information sharing and analysis center (ISAC). The Partnership for Critical Infrastructure Security (PCIS) and the Critical Infrastructure Assurance Office CIAO both are geared to coordination and support of your security. That has not changed but your industry is now supported to a higher degree by increases in oversight, technical assistance, R&D efforts targeted on your industry needs, and more information sharing with federal agencies.

What You Can Do Now

Study "*The National Strategy to Secure Cyberspace*" carefully and consider doing the following, not necessarily in this particular order:

1. Develop or revisit your enterprise security strategy that addresses threat management by installation of preventive controls, assurance the controls are effective, monitoring for inevitable failure of those controls, and planning for restoration and recovery from those failures.
2. Become active in the public and industry-specific debates about security and best practices.
3. Educate yourselves and your enterprise about what your threats and vulnerabilities really are. Use an outside and independent professional security service to help you bypass the internal politics that often interfere with the internal disclosure dialogue and the honesty this effort requires.
4. Start thinking in terms of creating an ongoing security process that proactively mitigates vulnerability management, not just fixing vulnerabilities discovered in audits (putting Band-Aids on a balloon). Restructure your organizations as needed or clearly allocate responsibilities to foster these new functions.
5. Think beyond managing only known threats. For example, the NIMDA virus mushroomed to global scope in less than an hour of its release, far faster than any organization could possibly respond to it.
6. Buy smart. Factor in security as a requirement and a cost. Don't buy technology or products that worsen your security problems and cost you more to secure them than the savings from increased productivity you were trying to achieve. Look at the ROI!
7. Establish an Incident Response Team, train and equip internal and external first responders now for the next major incident, don't wait for it to happen. Prepare for the possibility that your network may have been laced with backdoors for use in cybercrime, terrorism, industrial espionage, or cyber warfare. The largest number of attacks will come from the outside, but the most costly attacks will come from insiders!
8. Think global in scale. The defined network perimeter does not exist any more. Most networks are interconnected in ways and to parties that far exceed the original design and no single organization or technology controls those interfaces.
9. Don't use the "National Strategy to Secure Cyberspace" as a model for the enterprise. This is a plan for the Federal government to meet its needs and most certainly does not mirror your enterprise' needs. Create your own strategy to meet your own needs and acquire the assistance of a professional security services organization that can help identify those needs and devise a workable plan to meet them.
10. Don't wait for new international standards to guide the security strategy for your enterprise. The existing standards, specifically ISO 17799 are already mature and may well exceed your ability in implement them.

The Business Case – Where is the Return for this Investment?

The tremendous savings possible from use of cyberspace for business are hampered by lack of trust in those systems. Securing cyberspace will allow the continued realization of growth of those savings and synergy. Security measures will put into place the framework to perform modern network management that is more efficient and effective. Security measures reduce the opportunity for costly waste and fraud. The cost of severe cyber attacks generally far exceeds the costs that would have been required to prevent them to begin with. Security measures generally result in architectures that support remote access and customer or supply chain interactions that were not previously possible and expand efficiencies and business models accordingly.

Security must be thought of as another tool in our arsenal that will help us meet our goals and mission. Promoting security for security sakes is wrong, the reason we should be promoting security is that it will help us meets our goals and without security we will not meet those goals.

Appendix A - What the Strategy Calls For

"*The National Strategy to Secure Cyberspace*" identifies 24 strategic goals and 85 recommendations to develop a capability to better manage the threats and vulnerabilities of cyberspace. The strategic goals have the common premises that protection of the whole is obtained by empowering each to secure their own portion of cyberspace and that security efforts must evolve as fast as or faster than new threats. To achieve these goals, a set of six tools are provided. Each tool is a basic security best practice and consists of multiple goals generally appropriate to most businesses, agencies, and users. The call is for each citizen of cyberspace (people and organizations) to use the six tools to accomplish the specific recommendations and to use the goals as a roadmap to coordinate efforts with the other users/owners of cyberspace.

The six tools are:

1. **Awareness and Information (3 goals):** Educate and create awareness among users and owners of cyberspace of the risks and vulnerabilities of their system and the means to mitigate these risks.
2. **Technology and Tools (3 goals):** Produce new and more secure technologies, implement those technologies more quickly, and produce current technologies in a more secure way.
3. **Training and Education (3 goals):** Develop a large and well-qualified cybersecurity workforce to meet the needs of industry and government, and to innovate and advance the nation's security capabilities.
4. **Roles and Responsibilities (5 goals):** Foster responsibility of individuals, enterprises, and sectors for security at all levels through the use of market forces, education, and volunteer efforts, public-private partnerships, and in the last resort, through regulation and legislation.
5. **Federal Leadership (5 goals):** Improve Federal cybersecurity to make it a model for other sectors by increasing accountability, implementing best practices, expanding the use of automated tools to continuously test, monitor, and update security practices; procuring secure and certified products and services; implementing leading-edge training and workforce development; and deterring and preventing cyber attacks.
6. **Coordination and Crisis Management (5 goals):** Develop early warning and efficient sharing of information both within and between public and private sectors so that attacks are detected quickly and responded to efficiently.

The users and owners of cyberspace are a highly diverse group and their respective roles in securing cyberspace are likewise diverse. The goals and recommendations for using the six tools are presented to five different levels or categories, based on the usage type of the individual or organization and their respective needs. The general summary of the recommendations for each user category are:

Home users and small businesses (5 recommendations) - Defend yourselves by using good passwords, security software and frequent operating system maintenance.

Large enterprises (7 recommendations) – Voluntarily secure your own systems and products by taking ownership of the security problem at the highest executive levels, adopt basic security best practices, and inter into a partnership to share information with government agencies.

Government, private industry, higher education (19 recommendations) – Detailed directives and timetables for the use of technology, inter-agency cooperation, planning, and best practices to secure respective systems and support the private and enterprise users (private industry is considered the owners of nationally critical infrastructure and thus subject to special government support).

National Priorities (49 recommendations) – Comprehensive plan for soliciting voluntary cooperation from the private sectors at all levels, providing support for technological improvements to the components of the Internet (R&D effort), perpetuating existing programs and initiatives, and serve as an example for the rest of the cyberspace user/owner community.

Global issues (5 recommendations) - Directions for the Federal government to engage and support the global community to secure cyberspace and development of new international security standards.

The results of these efforts will hopefully be an assurance that "any interruptions or manipulations of these critical functions will be infrequent, brief, manageable, geographically isolated, and minimally detrimental to the welfare of the United States".

Appendix B – Seven Recommendations for Large Enterprises

1. CEO's should consider forming enterprise-wide corporate security councils to integrate cybersecurity, privacy, physical security, and operational considerations.

2. CEO's should consider regular independent IT security audits, remediation programs, and reviews of best practice implementations.

3. Corporate boards should consider forming board committees on IT security and should insure that the recommendations of the chief information security official in the corporation are regularly reviewed by the CEO.

4. Corporate IT continuity plans should be regularly reviewed and exercised and should consider site and staff alternatives. Consideration should be given to diversity in IT service providers as a way of mitigating risks.

5. Corporations should consider active involvement in industry-wide programs to: Develop IT best practices and procurement standards for like companies, share information on IT security through an appropriate information sharing and analysis center (ISAC), raise cybersecurity awareness and public policy issues; and work with the insurance industry on ways to expand the availability and utilization of insurance for managing cyber risk.

6. Corporations should consider joining in a public-private partnership to establish an awards program for those in industry making a significant contribution to cybersecurity.

7. Enterprises should review mainframe security software and procedures to ensure that effective technologies and procedural measures are being utilized, IT vendors and enterprises employing mainframes servers should consider developing a partnership to review and update best practices of mainframe IT security and to ensure that there continues to be an adequate trained cadre of mainframe specialists, and IT security audits should include comprehensive evaluations of mainframes