ISACA®
Trust in, and value from, information systems

3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008-3105, USA
Web Site: www.isaca.org

Telephone: +1.847.253.1545
Facsimile: +1.847.253.1443
E-mail: info@isaca.org

8 April 2013

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Re: Developing a Framework to Improve Critical Infrastructure Cybersecurity

To Whom It May Concern,

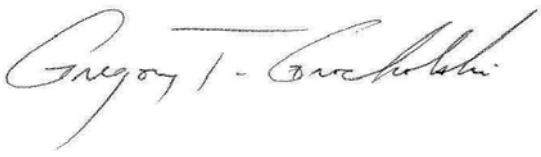
I am the international president of ISACA, a worldwide independent thought leader on information and systems assurance and security, enterprise governance and management of IT, and IT-related risk and compliance.

We applaud the US Government's cybersecurity focus and NIST's plans to develop a framework focused on helping to reduce cyberrisks. NIST's emphasis on the importance of a framework to help align business, policy and technology risks is particularly insightful. The proper control and use of an effective cybersecurity approach are critical to the economy of the United States and all global economies—which renders NIST's undertakings all the more important. Ensuring our workforce has the proper skills and capabilities continues to be a critical issue for governments as they prepare to move rapidly on their strategies.

The growing global importance of cybersecurity necessitates good governance over IT projects and systems. Regrettably, however, the importance of governance and the role it plays in sound cybersecurity strategies and policies is often understated or not addressed at all. The ability to run IT as a business, producing positive contributions as expected from other parts of an enterprise, is a critical success factor. Since cybersecurity aspects and implications are so integral to how enterprises operate today, a sound approach for evaluating, directing and monitoring—where results are shared with the respective units of government and other parts of the critical infrastructure—is an imperative.

ISACA appreciates the opportunity to assist where appropriate, and has provided more detailed comments below. We stand ready to provide other assistance to ensure that NIST's efforts to support a safe, yet reliable and robust, cybersecurity focus for the United States are successful and lasting.

Respectfully submitted,



Greg Grocholski, CISA, International President
ISACA (*www.isaca.org*)

About ISACA

With more than 100,000 constituents in 180 countries (40,000 in the US), ISACA members have developed, implemented, managed and assessed security controls in leading critical infrastructure organizations and governments on a global basis. ISACA is a leading global provider of knowledge, certifications, community, advocacy and education on information and systems assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. ISACA continually updates COBIT®, which helps IT professionals and enterprise leaders fulfill their governance and management of IT responsibilities, particularly in the areas of security, risk, assurance and control to deliver value to the enterprise. COBIT is used within many governmental departments and regulatory bodies around the world. ISACA also participates in the development of international security and governance standards through its global liaison status with the International Organization of Standardization (ISO).

Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations.

The Cyberprepared Enterprise: Frameworks That Promote Effective Cybersecurity

Introduction

The National Institute of Standards and Technology (NIST), in response to President Obama's executive order "Improving Infrastructure Cybersecurity," and in recognition of the Commerce Department's interest in helping American business to address cybersecurity issues and risk, is progressing a plan to develop a cybersecurity framework. This initiative is intended to provide a set of frameworks and best practices that can serve as a guide to critical infrastructure organizations. The material will enhance the capability of critical infrastructure enterprises to reduce the threat to the information, networks and computers that are vital to the nation's economy.

Developing a framework that will reduce risk to critical infrastructure entities and protect digital information and infrastructures from the full range of cyberthreats is an important step forward, given the increasing number and severity of cyberincidents. To be effective, however, the resulting NIST framework will need to address the complexity of cybersecurity. While the focus of the framework is cybersecurity, it should also address the need for enterprises to be profitable and to embrace innovation (business value needs to be preserved and not sacrificed). The framework and best practice recommendations need to be broad enough to address the unique characteristics of enterprises across different market segments. They also need to be useful, serving as a resource that both small and medium enterprises and industry leaders can benefit from equally.

To be effective, the framework and good practices must be adopted from the boardroom to the mailroom. Information and the information technology on which enterprises depend to manage activities, create products and serve their constituents touch every part of the enterprise. In every activity, a balance must be achieved among the value that is to be obtained, resource allocation and risk considerations. Since risk related to information and to information technology permeates the enterprise, solutions need to be part of the foundation of how enterprises plan and execute strategies and operational activities. Technical solutions cannot prevent attacks that exploit human and operational weaknesses. The failure to incorporate human, cultural and procedural elements as part of an enterprise cybersecurity capability will reduce the effectiveness of even the best technical solutions.

The following content presents ISACA's view of cybersecurity and references *de- facto* standards and frameworks ISACA has developed to assist enterprises in the governance and management of information and information systems. COBIT® 5 and related products, including *COBIT 5 for Information Security* and *Risk IT,* have been adopted and used by many National governments and private-sector organizations. Use of these references will help enterprises gain competitive advantage by guiding them in developing mature management processes that can be applied to cybersecurity.

Evolving World of All Things Cyber

Providing an effective means for enterprises to protect information and information systems from cyberthreats requires a forward-looking approach. Many of the technologies and practices currently in use were developed in an environment that is very different from the cyberworld of today and tomorrow. Identity and authentication mechanisms, tools to detect hostile actions, and mechanisms to protect systems were developed at a time when information technology could be contained within the walls of a data center. Internal and external connections to the enterprise were well defined, understood and threats blocked by firewalls and intrusion prevention systems. Patching systems provided reasonable protection against compromise.

However, information cannot be as easily contained with the growing use of mobile devices, ready Internet connections and global access in the cloud. The advent of smart interconnected devices multiplies opportunities for better performance and manageability while also increasing the number of targets that need to be protected from attack and compromise. With the evolution of technology and information protection and the increasing number of rich targets, there has been a shift from early, relatively unsophisticated attackers ("script kiddies") to skilled and well-funded adversaries who have the ability to conduct persistent, planned purposeful attacks. Technology has evolved so that everything has a cyber component. Threats driven by international economic competition, terrorism and cybercrime will require enterprises to address cybersecurity in a different manner.

We are currently at the starting point for changes in the application of technology and the general availability of information. Cloud computing, mobile devices, social media, analytics and the Internet of everything are already changing how individuals and enterprises create, use and benefit from information and technology. The mechanisms and approaches that enterprises use to protect their critical infrastructures and sensitive or personal information must anticipate a future in which everything is cyber.

A Cybersecurity framework, good practices and procedures that do not anticipate a very different future will fail, for those who depend on critical infrastructures and critical infrastructure enterprises themselves. A world in which every device has a network address, intelligence is built into machines and products, and vast quantities of information are collected and disseminated in the normal course of doing business requires protection that is built into how management plans and disseminates information and how technology is designed, built, and managed. An effective cybersecurity strategy needs to comprehend that:

- The cyberworld will require a change in how individuals and enterprises think about information and information protection.
- Taking a forward-looking approach to cyberprotection will provide long-term benefits.
- Cyberprotection strategies for enterprises need to be holistic, addressing the governance and management of information and information technology.
- Cybersecurity practices, processes and controls need to be defined, implemented and managed as a protection system rather than as individual measures.
- Technical cybersecurity solutions will fail if they are not integrated into a comprehensive program, since technology alone cannot address the complexity of cyberattacks.

As enterprises deploy technology to gain market advantage, and as consumers leverage technology to maintain relationships and to identify and obtain products and services they value, adversaries will increasingly seek out opportunities to exploit technical and operational weaknesses and subvert consumer trust to compromise systems for competitive or criminal advantage. A comprehensive, enterprisewide program for the governance and management of information and information technology, in which risk is identified and prioritized as an enterprise consideration, will be needed as a basis for developing effective management and technical cybersecurity programs executed by trained and capable staff.

The Governance and Management of Information and Technology

As previously stated, an effective cybersecurity program must address more than the technical aspects of risk. The technical measures required to manage cyberrisk need to be connected to the governance and management structure of the enterprise. It is within this structure that the goals of the enterprise are established and resources are made available to advance the strategy and to

sustain the enterprise. A technical cybersecurity program that is not integrated into strategy and resource planning is likely to be ineffective, under-resourced and of low priority. They risk becoming after-the-fact considerations.

When cybersecurity is considered within the governance and management structure of the enterprise, a culture of security is fostered throughout the enterprise. The organizational structure optimizes cybersecurity planning and execution, policies and processes enforce the assignment of cybersecurity roles and responsibilities, and cybersecurity thinking and actions are integrated as a part of how the enterprise operates. People with needed skills and expertise are available to the enterprise and supported through a workforce that understands the importance of cybersecurity and integrates cybersecurity practices into daily activities. Effective integration of cybersecurity into the governance and management structure of the enterprise ensures that security is connected to the enterprise mission, values and priorities—a connection that is integral to the program's success.

An internationally recognized *de facto* standard, COBIT® 5 (www.isaca.org/cobit5) provides the structure required for the effective governance and management of information and information technology and addresses the need for cybersecurity programs to be connected to enterprise goals, values and priorities. It has been continually developed and supported in collaboration with international experts, and is already embraced by many governments and industry organizations—including many organizations considered to be part of the critical infrastructure.

COBIT's goals cascade provides a way of specifying information and information technology goals starting with stakeholder needs, then leading to enterprise goals and to IT goals. The goals cascade also connects to enablers, which include principles and policies, processes, structures, and enterprise culture, as well as resources such as people, skills and competencies; service infrastructures and applications; and information.

COBIT® 5 also provides a process reference model that specifies 37 governance and management processes, and identifies IT-related goals, activities, process metrics and recommended inputs and outputs related to each process. As a governance and management model, COBIT® 5 provides a common language and approach that enterprises can use to plan and prioritize cybersecurity program activities across the multiple business units that will need to engage in cybersecurity as users or providers of protection programs.

Cybersecurity and Enterprise Risk Management

Information and information technology are at the center of how enterprises manage activities and serve stakeholders. A lapse of security can have consequences that impact immediate operational capabilities, affect the reputation of the enterprise, compromise the ability to satisfy regulatory or contractual requirements, and constrain effective support of strategic relationships. Due to the harm that can result from a cyberattack, and the level of dependence enterprises have on information and information technology, cyberthreats need to be addressed as an operational risk with enterprise consequences. This understanding escalates the importance of cybersecurity to something much greater than a technical risk. It is an enterprise concern, and must be addressed on an enterprisewide basis.

While technical exploits contribute significantly to cybersecurity concerns, attackers have been very successful leveraging every avenue to gain unauthorized access to protected resources. Since human factors, culture and internal practices can be as effectively manipulated as program errors and misconfigured devices, cybersecurity programs need to address these vulnerabilities.

Managing operational risk related to cybersecurity as an enterprise risk requires a business-oriented management approach, to provide a common view across the enterprise and support risk-aware business decision making. *The Risk IT Framework* (*www.isaca.org/riskit*) takes that business-oriented view by addressing cybersecurity through three domains: risk governance, risk evaluation and risk response. Each domain contains three processes that specify key activities within the process, information flows and performance management recommendations. The Framework provides a COBIT-linked reference model for addressing cyberrisk, in a systemic and holistic manner, so the efforts of all those within the enterprise who need to be engaged in risk determination and management are effectively engaged. To enhance the ability of enterprises to govern and manage enterprise IT and to integrate risk management from a business strategic and operational perspective, ISACA will be releasing *COBIT 5 for Risk* in the 4th quarter of 2013. This volume will provide a risk focused perspective for the COBIT 5 framework.

Cybersecurity Program Management and Execution

When cybersecurity is integrated into how information and information technology are governed and managed, and risk is identified and prioritized with an understanding of the potential for harm to the enterprise, the real effort of cybersecurity will fall upon those who are responsible for the enterprise security program. The program is not a special segment of information security. As the world becomes more cyber than legacy in orientation, cybersecurity and traditional security blend. There can be no division between cybersecurity and information security efforts since there can be no distinction between the technology that will be required to protect enterprise information and information system infrastructures. Those who are intent on compromising systems do not think in terms of legacy and cyber. They focus only on what they need to be successful.

Cybersecurity program activities and the priority for implementing required components must be aligned with stakeholder needs and organization goals. These set the cybersecurity environment and establish enterprisewide urgency for cyberinitiatives and programs. Stakeholder needs and organization goals also define the extent of risk that the enterprise is willing to assume and the investment in protection that is appropriate. Policy, standards and guidelines define roles and responsibilities and establish the enterprise environment within which the cybersecurity program will be developed and executed.

A cyberworld may require more focused efforts and greater integration of security into both enterprise and technology management activities. It may also require the development of different tools and enhanced capabilities that need to be implemented to account for increased threat levels and persistent attacks. Roles and responsibilities may need to be refocused. Policies may need to be revisited. Budgets may need to be augmented. An initial step in making the transition from a legacy-oriented information security program to one that is cyberfocused is determining the extent of the gap that exists and how this gap can best be filled. Making the transition to a cybersecurity-focused protection program will require effective change management.

COBIT® 5 for Information Security (www.isaca.org/cobit5security) provides a security perspective drawing on the COBIT 5 framework content and guidance. The COBIT 5 principles, enablers and implementation guidance are enhanced with security-specific content that will benefit the formation and management of a cybersecurity program.

Cybersecurity Staffing and Preparedness

A comprehensive cybersecurity program requires that those who gain value from information and information technology resources provided by the enterprise can trust that systems are secure,

compromise attempts can be detected, and, in the event of an intrusion, recovery is quick and complete. Achieving the level of required trust will depend on the availability of qualified and capable specialists who can manage and execute the cybersecurity program.

As part of the National Initiative for Cybersecurity Education, a framework to develop a national cybersecurity workforce was developed. This framework identifies professional roles encompassing the need to securely provision technology solutions, to operate and maintain these systems, to protect and defend them from misuse and compromise, and to investigate suspicious or wrongful activities when they occur. The framework also recognizes the need to provide oversight and guidance for the development of the cybersecurity program. These professional roles and positions within these categories define roles that need greater focus as well as those that may already exist without a specific focus on cybersecurity. The defined roles and responsibilities broadly address professional activities from information systems operations, application development, systems engineering, systems architecture, and specializations in information systems assurance and protection. To meet the cybersecurity challenge, existing personnel in roles impacting cybersecurity performance will need to gain those additional skills required within their current work assignments. Gaining the required skills and applying them in the performance of their positions will be enforced within the culture change that is necessary to address cyberrisk in a more holistic manner. This becomes an imperative as cybersecurity and risk management are elevated to an enterprise priority.

A framework such as the Skills Framework for the Information Age (www.sfia.org.uk) can be useful to manage skills acquisition. This international skills and competency framework describes IT roles and the skills needed for them. It categorizes technical positions according to strategy and architecture, business change, solution development and implementation, service management, procurement and management support, and client interface. Each position in the framework is assigned a level related to the position's autonomy, complexity, influence and business skill requirements.

In addition to managing position and skill levels, enterprises need to be assured that individual workers have attained the skills required for their position. Learning-based certificates and competency-based professional certifications can be used to enable management and individuals to attest to their capabilities. The Certified Information Security Manager certification (www.isaca.org/cism), based on job task analysis documenting the critical activities and knowledge required to effectively implement and manage an information security management program, is an appropriate professional credential for those who will be charged with leading a cybersecurity program. The Certified in Risk and Information Systems Control certification (www.isaca.org/crisc) is similarly based on a job task analysis renewed every five years. It is suitable for those who will need to lead a cyberrisk program that encompasses technical cyberrisk considering the operational impact within the context of enterprise priorities. Ensuring that cybersecurity programs and business strategy are aligned, the Certified in the Governance of Enterprise IT (www.isaca.org/cgeit), certifies that professionals with this designation are capable of directing and implementing a comprehensive program that addresses traditional IT integration into the enterprise but also the need for cybersecurity activities integration into enterprise activities. Lastly, the Certified Information Systems Auditor (www.isaca.org/cisa) attests to the capability and credibility of those who need to provide management assurance that cybersecurity practices are effective and efficient by managing and executing cyber focused information systems audit programs.