Information Technology &
Communications
Sector Coordinating Councils

March 20, 2009

Ms. Melissa E. Hathaway
Acting Senior Director for Cyberspace
National Security Council/Homeland Security Council
The White House
Washington, DC 20500

Dear Ms. Hathaway:

The Information Technology Sector Coordinating Council (IT-SCC) and the Communications Sector Coordinating Council (C-SCC) are pleased to provide this joint response to the White House's 60-Day Cyber Review. As the primary industry segments responsible for various aspects of IT and Communications security, we recognize that we have a special obligation to assist the Administration in its review of cyber matters and to articulate the important role of both government and industry in protecting the nation and its resources from malicious cyber activity. In this letter, we respond specifically to the four questions that were posed to both Councils and have attempted to be both concise and comprehensive in our answers.

- *What is (should be) the government's role in securing/protecting the critical infrastructures and private sector networks from attacks?*
- *Do you have thresholds for reporting cyber incidents?*
- *How much of your budget gets set aside for cyber/IT security?*
- *Can we create an index that would measure how one country compares with another in terms of a "digital index" or a country's "digital maturity"?*

We also understand from our discussions with you two weeks ago that it may be appropriate to schedule a follow-up meeting. This may afford you an opportunity to gain further elaboration or clarification from us, as well as an opportunity to share with us what you have learned. In addition, we would be pleased to offer any assistance you may need in your evaluation of the myriad sets of recommendations you are receiving regarding cyber security.

On behalf of both the IT and Communications Sector Coordinating Councils we once again thank you for your eagerness to seek industry input and we look forward to supporting your efforts and those of the Administration as these vital efforts evolve.

Best regards,

Robert B. Dix, Jr.
Chair
Information Technology
Sector Coordinating Council

Robert Mayer
Chair
Communications
Sector Coordinating Council

Information Technology and Communications Sector Coordinating Councils

Response to White House Cyber Review Questions

March 20, 2009

In order to develop these responses, the Information Technology and Communications Sector Coordinating Councils, as part of their consensus processes, sought comments from corporate and organizational members of the Councils. The comments received were synthesized into ranges of answers for use in these responses. Accordingly, any particular statement in these responses may not represent the view or situation of a particular member.
The information contained in the response to Question 3 was provided to various members of the Councils under their independent contracts with third-party consultants. These contracts do not allow this information to be publicly distributed without prior express consent. Should you wish to make public the response and the associated appendices, please advise the Chairs and we will endeavor to obtain the necessary permissions

1.0 ROLE OF THE GOVERNMENT

What is (should be) the government's role in securing/protecting the critical infrastructures and private sector networks from attack/damage (e.g., from nation states)? Intended Direction: Address the Government's role in securing cyber CIP in terms of "people," "process," "technology," "regulation," and "incentives."

The sectors have identified the following recommendations regarding the role the government should take to secure and protect private sector critical infrastructure and key resource (CIKR) networks. Already, a reservoir of organizational trust and established working relationships throughout the critical infrastructures exists; this reservoir is ready to be utilized as the spring board for generating future successes in this area.

1.1 Support and strengthen ongoing public-private partnerships to improve threat and vulnerability collaboration and information sharing

1.1.1. Public-Private Partnership

In order to successfully collaborate with the private sector, the Government must create a strong foundation on which a trusted partnership can be built upon and nurtured. Some imperatives required to create a trusted environment and effective partnership in this space include having the following in place:

- Value propositions understood by both Government and industry partners
- Controlled communication mechanisms for the sharing of information
- Government facility access for relevant on-site collaboration in support of the trusted partnership model

Administrative, logistical, cultural and physical roadblocks continue to hamper the creation of the functional collaborative operating environment needed for the partnership model. The inability to overcome these roadblocks undermines the government's stated objective of a private/public partnership. To build a trusted environment, both public and private sector individuals need face to face interaction and thus access to facilities/buildings where collaboration can take place regularly. When geography prevents face to face interaction, virtual collaboration via controlled communication mechanisms is necessary to foster a trusted environment (i.e. secure conference bridges and portals). These practices are the foundation upon which a partnership is established, grows, matures and functions. Overlooking these fundamental areas will only hamper progress.

A variety of collaborative mechanisms exist relating to both the policy and operational dimensions of cyber security. The government and private sector should review the relative

effectiveness of existing mechanisms and encourage the further development/expansion of those that have produced the most significant tangible results.

1.1.2 Threat and Vulnerability Collaboration and Information Sharing

The Government is uniquely positioned to coordinate intelligence collection and analysis, and provide threat and vulnerability information to the private sector, including both classified as appropriate, and "sanitized" as necessary. This sharing of information will facilitate improved implementation of protective measures in an effort to more effectively manage risk. Although the private sector uses a number of sources and means to gather threat and vulnerability information, a strong and continuing government commitment to collaborate with the private sector to identify necessary information sources and to coordinate on the collection, analysis, and sharing of such data in real-time, would be of the utmost value in prioritizing actions and resource allocation to secure CIKR networks. To assist in achieving this desired environment, the sectors encourage Government to continue to sponsor relevant private sector partners in the clearance process.

While there are a number of initiatives between the government and private sector to develop processes and protocols to provide this information, the IT and Communications Sectors believe that government remains uncomfortable with this concept, even at a sanitized or "tearline" level. The "discomfort" associated with government-to-private sector sharing needs to be addressed affirmatively at the highest levels of government to move forward with an operational information sharing framework. At the same time, the relationship and collaboration from the private sector to government must also be addressed to achieve a true bi-directional collaborative and integrated capability.

To achieve an operational and collaborative information-sharing framework that identifies critical cyber security priorities, works to implement those priorities in a transparent way, and tracks progress to promote accountability for meeting those requirements, the IT and Communications Sectors recommend that government representatives at the highest levels work with private sector representatives within the Critical Infrastructure Partnership Advisory Council (CIPAC) framework to:

- Define a clear and coherent set of national cyber security strategic objectives;
- Describe information sharing objectives related to situational awareness, analysis, prevention, detection, mitigation, response, and recovery;
- Assign clear roles to entities to focus the Nation's efforts, drive resources and action, and promote accountability and responsibility;
- Remove and address any existing or perceived legal and/or regulatory barriers that may restrict or inhibit information sharing;
- Promote collaboration and bring stakeholders together to address a variety of topics, including threat targets, tactics, and methods (not sources) and attack scenarios; response procedures and actions; vulnerabilities and technologies to mitigate the exploitation of

current and future vulnerabilities; a national cyber risk assessment; and cyber security requirements;
- Engage with sector designated operational entities to define operational requirements and procedures, and implement a working, operational capability and/or enhance those that currently exist.
- Prescribe timelines for achieving the above activities.

The Government provides assistance to the private sector in securing CIKR networks through information sharing and facilitation, and through support of mechanisms (e.g. public-private partnerships) to integrate private sector information and situational awareness into the decision making process (either in policy or operational activities). There are many situations, however, where the Government may provide more direct assistance (e.g., operational response teams, resources under the National Response Framework, etc.) to the private sector. Although larger organizations may have sufficient in-house capabilities to address their cyber security needs, smaller organizations may require assistance (at varying levels) from the government to assess and respond to incidents.

1.2 Fundamentally change the Cyber Security operating environment

1.2.1 Incident Management

The government and industry need to come to an agreement and adopt a philosophy on what constitutes as an incident that reaches the magnitude for triggering a mechanism for a joint response (i.e., a cyber incident of national significance). Once that is defined, we believe that during a cyber incident requiring a joint response, Government should perform the following functions:

- Facilitate incident management of the event by a single Government entity with involvement of only those organizations that are directly involved in responding to and resolving the incident; and
- Facilitate the distribution of situational awareness to the rest of the nation for the purposes of facilitating the management of the consequences of the incident.

For cyber attacks sponsored or perpetrated by a nation state for which the Government has national security responsibilities, Government should ensure that a single Government entity is identified to pursue the appropriate course of action to address the perpetrator and has the proper authority required to do so. The Government also needs to clearly identify roles and responsibilities of the government organizations with equities in cyber security.

1.2.2 Malicious Actors

The IT and Communications Sectors would like to see all key government stakeholders, including but not limited to, law enforcement, trade and diplomacy, military, intelligence community, finance, business, and others engage with the private sector in a strategic effort –

both nationally and internationally – to proactively identify the most significant malicious actors in cyberspace, take appropriate action to end or block their activities, cut-off their funding, bring down black market sales of key vulnerabilities and exploit tools, and provide a feedback loop to policy makers to influence effective practices, standards, and research and development (R&D). These measures should be taken in addition to ongoing efforts to actively seek out and prosecute the individuals perpetrating cyber attacks.

1.2.3 Promoting Cyber Security Best Practices

To improve cyber security across the CIKR sectors, incentives should be provided for the adoption of effective security practices. Various activities have previously identified a series of recommendations and other activities are currently underway. Some of these incentives that should be examined and further explored include:

- As a customer, government should clearly articulate cyber security requirements in procurement activities. By specifying requirements in the procurement process, security will be "built in" from the beginning as products and services are developed and delivered to the government.
- In addition, cyber security requirements should be included in provisions associated with the distribution of public funds to states, local governments, and others, such as in the case of federal grants and eligibility for Stimulus Package funds.
- Government should work with industry to examine additional opportunities to leverage the purchasing power of the federal government to catalytically influence improved cyber security practices.
- The government should work with industry and academic standards organizations to examine the need and benefit of developing, promulgating, and requiring the use of standards for the systems and networks (e.g., SCADA systems) that manage critical infrastructure.
- The government should look toward existing public private incentive programs such as the SAFETY Act to create a Cyber SAFETY Act. Limitation of liability protection would be afforded to companies who have exercised approved security practices.
- The government should examine alterations to the Stafford Act to encourage greater public private cooperation in times of crisis.
- The government should enhance Small Business Administration loans for small business vital to the critical infrastructure to facilitate needed expenditures to improve overall cyber security which may not otherwise be justified as a core business investment.

1.2.4 Training and Education

Besides incentives for industry, the IT and Communications Sectors recommend expanding and enhancing a national-level cyber security awareness program to inform three distinct communities of users: 1) K-12 education, 2) Higher education, and 3) Individual and small business users. This will go a long way towards improving the Nation's cyber "health," not only by improving user education, but by bringing cyber security into the public's view on an elevated and sustained basis.

In addition, the IT SCC recognizes the importance of creating and maintaining a world class cyber security workforce—in both the public and private sectors. To achieve this goal, the government must seek to establish its own workforce as the model for competence and professionalism. Specifically the government should recognize that cyber security has become a separate, distinct career field and establish a unique job series for this profession within the federal civilian personnel system. This will have a corresponding positive effect throughout the other components of the public sector, and possibly enhance the status of IT security practitioners in the private sector.

Finally the government should seek to significantly enhance cyber security professional education programs at the nation's colleges, universities and community colleges to ensure that there is a continuing flow of qualified individuals entering this important career field.

1.3 Fund Cyber Security Research and Development

The IT and Communications Sectors recommend that cyber security research and development (R&D) and funding for cyber security-related R&D initiatives and projects be made a national priority. Additionally, the IT and Communications Sectors recommend that national cyber R&D priorities should be identified and incorporated into a national cyber R&D plan with specific requirements and objectives informed by work completed and underway by the government, private sector and internationally. Public-private partnerships will be crucial to maintaining the level of cyber R&D needed to make these changes a reality. To date, the Government – particularly at senior levels – is not sufficiently involved in the coordination of R&D efforts. The sectors recommend continuing R&D coordination efforts under the Comprehensive National Cybersecurity Initiative (CNCI) and IT Sector Research and Development Working Group. More broadly, these efforts should be expanded through cross-sector groups to address the cyber R&D needs of all 18 CIKR sectors. As stated above, this effort should culminate in a national cyber R&D plan.

1.4 Develop an International Cyber Security Strategy and Ensure Interagency Coordination

The Government is also responsible for representing the citizens of the United States in international technical, legal, and diplomatic forums and debates. While the Internet is certainly a shared resource between the public and private sectors, the Government has a unique role in diplomacy, international law, and global politics that cannot be delegated to the private sector. It is imperative that the Government engage other countries and become a leader in international debates pertaining to the future of the Internet, and its impact on the global economy and security. International coordination should extend to the diplomatic and international law domains, but also into the coordination of the policies required to support new capabilities in a globally distributed next generation network (NGN) environment. This coordination effort is particularly important when the United States is engaged with domestic and international policy and standards entities to develop a more consistent, unified U.S. strategy to enhance current agency activities.

For example, as part of an international cyber security strategy, the Government must find ways to more effectively leverage engagements with key partners and the global community as a whole (perhaps at varying degrees, as appropriate) to collaborate on improving situational awareness, analysis, and response and recovery measures.

In addition, the strategy should articulate where in the international community the Government should engage and with what position(s), as well as address the role/efforts of the agencies engaged to ensure a consistent and coordinated approach. The private sector is a critical stakeholder in these efforts and the Government should engage with the private sector whenever possible and appropriate.

1.5 Ensure that cyber security and the national security (NS) mission of the National Communications System receive the proper level of visibility and support

Cyber security is vital to our nation's economic stability and prosperity. Defending against attacks and keeping our critical functions secure should receive the proper level of visibility within the Government. The IT and Communications Sectors recommend that a senior policy advisor for cyber security be located at the White House. The advisor's charge would be to provide coordination across the federal government and with the authority to demand accountability; drive collaboration; promote information sharing; and provide the situational awareness critical to address cyber incident management and improve interagency coordination.

It is imperative that the national security work associated with the National Communications System (NCS) be given a substantially elevated and immediate priority with cyber infrastructure being declared a strategic asset. The NCS mission extends along a continuum from National Security at one end to Emergency Preparedness at the other. In recent years, DHS NCS has been focused on supporting DHS' emergency preparedness role in the wake of Hurricane Katrina. While this is important work, the NCS has not had the opportunity or resources to appropriately focus on the plans and programs necessary to address the National Security telecommunications needs of the country. Government needs to ensure that it engages with the proper National Security partners within the private sector to address cyber incidents.

Government should ensure that appropriate funding is allocated to the Communications mission/NCS, as an underlying infrastructure for cyberspace. Significant erosion of NCS funding is impacting its ability to support its mission.

2.0 CYBER INCIDENT REPORTING

Question 2: Do you have thresholds for reporting cyber incidents? Is there a particular threshold for reporting incidents to the "C-Suite," the Board of Directors? How do incidents get escalated? At what point do you inform the government?
Note: A discussion to clarify the question noted that government does not have these thresholds defined.

The Communications Sector Coordinating Council (C-SCC) and the Information Technology Sector Coordinating Council (IT-SCC) jointly polled member companies in response to the ongoing White House 60-Day Cyber Review. The poll included questions intended to determine what criteria are, or should be, used to determine when cyber incidents arise to a level of potential significance that warrants attention of national law enforcement, public safety, and/or national security officials. While necessarily limited in scope, there were questions aimed at determining if respondents have basic thresholds for reporting and responding to cyber incidents internally and externally, whether to law enforcement, other government organizations including national security, and/or private sector entities.

2.1 Poll Results Overview

While the received sample was small, the scope of significance of the responding companies to cyber security is large. Generally, the responding companies have a process to report a security incident internally. In most cases, if an incident becomes a security event, a documented means exists to handle it. Within this process, there are thresholds for reporting incidents to various stakeholders depending on the severity. Most companies have security events rated on various scales depending on the severity to the company. While most companies agree that the escalation process is dependent on the situation, reporting to senior management of the company, including the board of directors is limited, usually to those incidents creating a larger or externally visible impact. Most importantly, escalation to include reporting to the federal government is not likely unless the company believes it needs outside help or has a specific obligation to share (*e.g.,* Defense Industrial Base Initiative Framework Agreement).

2.2 How Incidents are Escalated

In general, companies reported having defined procedures for incident escalation. However, a wide range of options described various procedures from internal incident management policies and guidelines, to full bore incident response plans. Nearly all companies reported having a defined process for notifying affected internal customers. Thereafter, escalation protocol varied from a "judgment call" by the corporate security officer, to incidents escalating through the company's computer security incident response team processes. Some companies reported a

level of automation and escalation protocol based upon a rating methodology including the severity, risk, or in one example, a financial materiality assessment. Some companies described the ability to increase or decrease the incident rating severity as the event plays out in real time. There were examples of well-defined identification of internal stakeholders.

A best practice included documented incident response procedures for engaging the proper stakeholders to respond and resolve incidents, including IT managers, business managers, legal, public relations, human resources and corporate executives depending on the scope and impact of the incident. Another emphasized security education that included a training and awareness program providing the basis for reporting. Most companies reported having robust incident handling processes that follow a well-defined internal escalation process determined by predefined thresholds based on scope and impact of the incident. Cited sources for defining incidents included National Institute for Standards and Technology (NIST) guidelines.

There were some general ideas contained within the comments of the poll that point to differing goals for company escalation processes and reporting. On the one hand, companies follow a financial materiality assessment that is generally understood to be the legal department's responsibility and part of the traditional Securities and Exchange Commission (SEC) reporting requirements. On the other hand, companies more integrated into the critical infrastructure protection mission space indicated greater adoption and interplay with the incident response coordination mechanisms contained within the public-private information sharing framework.

Responses again differed on how companies interface with the various information sharing mechanisms to help inform the overall escalation process. For example, one company rarely needs to escalate an incident to an outside entity; however, in the extreme when they seek outside information, they contact the Network Security Information Exchange (NSIE) or use the secure United States Computer Emergency Readiness Team (US-CERT) portal. Some report incidents through their membership in the National Coordinating Center (NCC) for Telecommunications as another avenue to obtain and share incident awareness. Others point to the Information Sharing and Analysis Centers (ISAC), supported by both the IT and Communications sectors, as a key resource.

2.3 External Notification

While internal notifications appear to be generally well understood, respondents differed significantly with respect to when and how to notify external stakeholders. External notification scenarios can be described as escalations to the appropriate law enforcement agency depending on severity, scope, and jurisdiction of the incident. Incidents of a non-criminal nature are escalated based on a combination of factors such as severity, scope, or availability of risk mitigation controls. The external escalation path also varies based on several factors and may go through many and multiple channels, including national security and homeland security channels.

2.4 At What point do you advise the Federal Government?

The responses to the question of when companies advise the federal government varied widely. One company reported that no process exists for informing the federal government. Another reported ongoing conversations with the federal government on a range of security issues and risks, but do not currently report incidents on a regular basis. Improvements to information sharing with the federal government occur if the company is engaged in contracts providing services to the government as a customer. If there are impacts to services provided to the government, then the appropriate team would manage that communication.

Typically, the federal government is advised when required by to do so by law; for example, if an incident investigation requires engagement from law enforcement. Due to the potential complexity and constantly evolving nature of cyber incidents, some companies have taken a risk management approach to incident response and escalation with a predetermined range of factors influencing how and when incidents are escalated to various stakeholders. Clear examples for notification of federal authorities include when the issue impacts a contract or service provided to the government; when the issue relates to a loss or affect on the company that may require law enforcement to investigate and prosecute; and when an incident threatens to disrupt critical infrastructure or services.

2.5 Industry Recommendations for Thresholds

Caution must be exercised when attempting to set discrete thresholds due to the complexity and evolving nature of cyber threats and vulnerabilities, as well as the spectrum of potential impacts for a wide variety of enterprises. Recommendations include a comprehensive risk management approach that would enable the appropriate resources to be applied, at the appropriate time, to reduce the impact of the incident without negatively impacting the flexibility and agility of the responders. As it is difficult to diagnose the exact source and intent of an incident, it is imperative that thresholds be defined based upon historical incident data and monitoring of day-to-day cyber news and events by organization experts. In addition, incident reporting guidelines should be part of each organization's incident reporting and response plan. These thresholds should be published for use within an organization such that they are well-known and usable by staff at all levels.

Companies recommend some caution in the government over gathering routine incident information which may create undue burden on business and open business to legal risks without sufficient safe harbor. Government and the private sector should further explore the extent to which it would be worthwhile to record cyber incidents or related data and how long an organization should hold that data for potential post-incident analysis contribution. Industry should only report current incident information to the Government where existing law or regulation requires such reporting.

Additionally, the Government should be required to protect this information as "Protected Critical Infrastructure Information" (PCII). One responder suggested a Clearinghouse with

anonymous aggregation of reporting to provide visibility to private sector cyber incident response organizations. While current laws and regulations govern loss reporting, a consistent federal standard could be helpful rather than a patchwork of state and local legal requirements, that is, losses generally meet a standard of financial materiality (under Sarbanes-Oxley, typically $.01 per share), which public organizations would normally report in SEC filings. National security and public safety should always be a requirement to escalate reporting and response; however, the intended impact or motivation of an attacker may be difficult to determine during an attack or incident.

A consensus seems to be that a lack of clarity exists pertaining to how specific thresholds could be established without more information with respect to the types and scope of incidents and impacts of greatest concern to Government. In a perfect world, industry would report incidents that appear to be attacks against the infrastructure, or that appear to be significant in breadth and scope, or that appear to be from a nation state or radical group. As a practical matter, before that happens, industry and Government would need to address relevant issues such as indemnification, confidentiality, and reciprocity assurances.

2.6 Other Recommendations

Network and IT system owners and operators see a huge volume of malicious traffic every hour of every day. Because of this large amount of "background noise" efficient techniques need to be developed that enable workers to extract the critical information in the midst of this noise. Once armed with that critical information, an equally critical need persists for well-defined plans, policies and procedures to report cyber incidents within each organization. Also, reporting of cyber incidents needs to be tied to the unique requirements of each sector and each enterprise (*e.g.*, IT sector, financial sector, energy sector, etc). Even an enterprise may have more than one set of thresholds and response procedures. For example, an enterprise may own and operate extensive global, internal networks while simultaneously maintaining responsibility for supporting a huge base of clients of their products worldwide. Incidents could occur in either sphere and require different thresholds and response procedures. Others may have outsourcing clients and be committed to specific contractual arrangements with each.

As for reporting incidents to the federal government, guidelines and procedures must be defined and set forth such that workers at all levels of an organization are able to discriminate between incidents that are minor and those that are major (and all incidents in between) and to escalate appropriately. This capability requires a well-defined cyber security education, training and awareness program. The program must emphasize an awareness of prevailing threats, how those threats affect the specific sector, and the policies and procedures employed for reporting an incident. An indications and warning system with solid lines of communication – from the worker level to the C-suite to the federal government – is required. A delay in reporting at any level can result in a cyber catastrophe that could take days, weeks or months to recover from.

3.0 CYBER SECURITY BUDGET

Question 3: How much of your budget gets set aside for cyber/IT security?

Several major global consultancies routinely track various aspects of IT deployment by public and private enterprises. As information security concerns become more prevalent for executives and managers at all levels of an organization, analysts strive to examine the nature and drivers of security related investments. The White House has asked the Information Technology Sector Coordinating Council (IT-SCC) and Communications Sector Coordinating Council (C-SCC) to provide information on the overall budget and/or IT budget that is typically allocated to cyber security.

To obtain the broadest set of inputs and also leverage the significant work that has been conducted in this area, we obtained proprietary information that has been recently analyzed from The Yankee Group, The Gartner Group, Forrester and IDC. The attached analyst reports have been authorized for use by the IT-SCC, C-SCC and the White House. As detailed in these reports, the analyst community typically determines an organization's security percentage based upon a company's IT budget, rather than its overall budget. However, should the White House choose to determine percentage of security from the overall budget, one can identify what companies typically spend on IT as a percentage of their overall budget and thereby extrapolate the security percentage. It is the hope of the Councils that the team conducting the 60-Day Cyber Review will find the information that is presented helpful to their inquiry.

Finally, we offer the caveat that the information provided here was obtained through third party surveys that we have not independently validated. We do, however, take notice of similarities with respect to the information reported from the various sources and we are confident that the body of information contained in the reports is representative of industry trends.

NB: The information contained in the response to Question 3 was provided to various members of the Councils under their independent contracts with third-party consultants. These contracts do not allow this information to be publicly distributed without prior express consent. Should you wish to make public the response and the associated appendices, please advise the Chairs and we will endeavor to obtain the necessary permissions.

3.1 The Yankee Group

In October 2008, The Yankee Group ("Yankee Group") conducted a survey of 300 IT decision-makers representing U.S.-based enterprises with 500 or more employees.[1] Per the data, more

[1] See Appendices A, B and C.

than two-thirds of respondents have offices outside the U.S., and over 55% of the respondents who knew their IT budget indicated that they spend $1 million or more on IT computing infrastructure with the mean budget at $30.3 million. See Figure 3.1.

Approximately what percentage of your organizations IT budget is allocated to the following sub-categories?

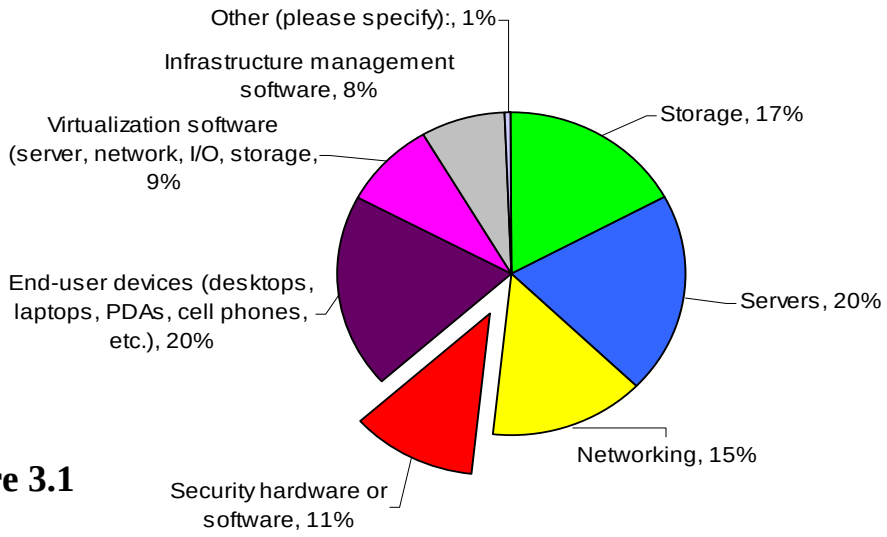

Figure 3.1

Respondents indicated that they spend approximately 11% of their 2008 IT infrastructure budget on security hardware and software. Yankee Group did not capture the associated IT operating expenses for these organizations and therefore the percentage that represents security hardware or software (11%) is less than the total cash outflow for the year.

Phil Hochmuth, a senior analyst at Yankee Group notes that:

> *Yankee Group believes that the average IT expenditure on enterprise security hardware and software (11%) is a conservative representation of the overall importance of IT security in the minds of enterprise technology executives, as that percentage does not include solutions and services used by compliance, data loss prevention, or managed security services. Security enhancements and expansion plans are a top priority among most enterprises; this means that security is now a factor in the decision-making criteria enterprise IT executives use when evaluating all categories of IT infrastructure equipment, from servers and storage, to networking, and endpoint devices.*

As seen in Figure 3.1.1, below, respondents also indicated that they prioritize network security infrastructure products with security enhancements, business continuity and recovery, and availability of applications and data topping the list.

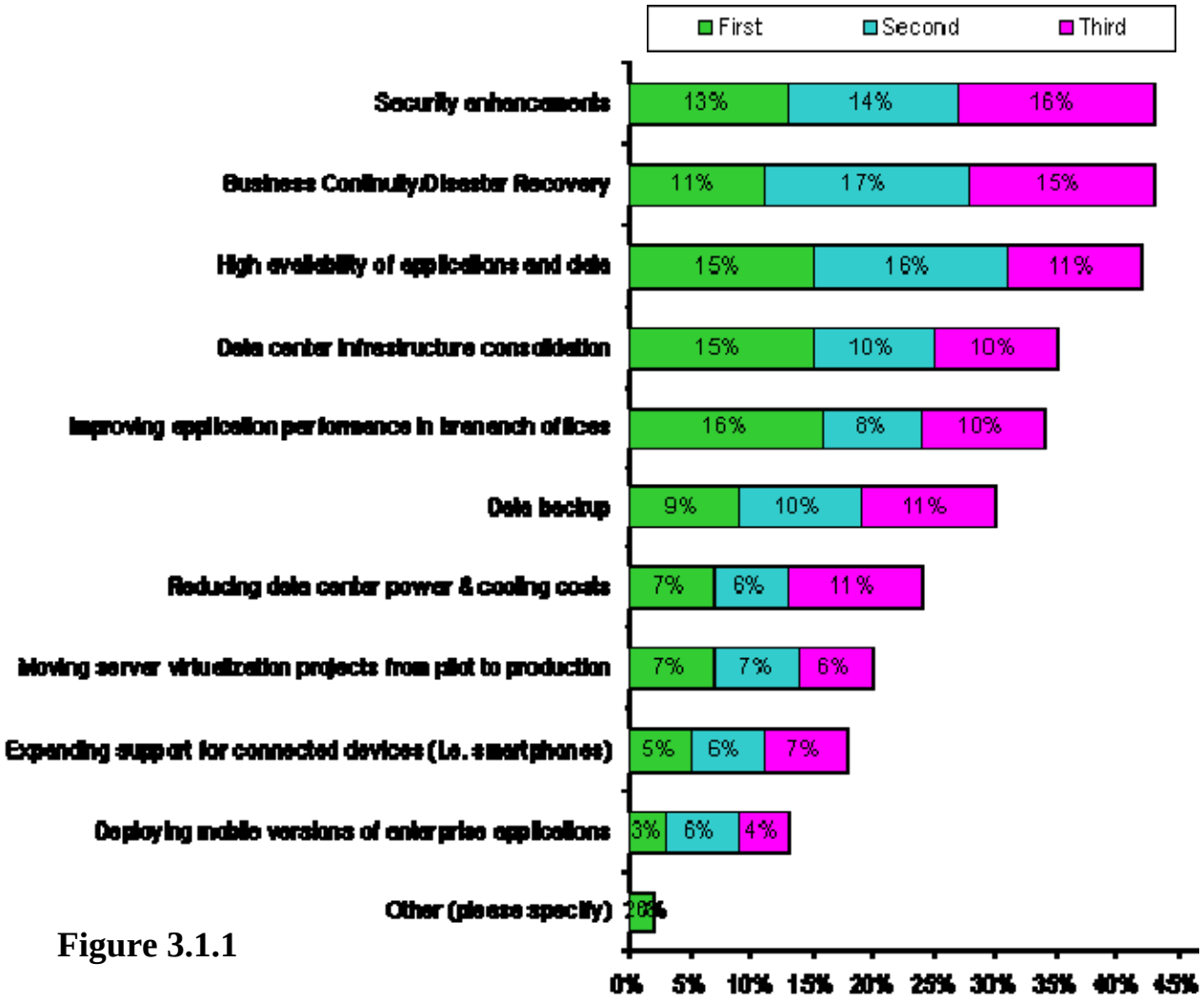

Figure 3.1.1

The Yankee Group study confirms that enterprise organizations continue to prioritize protecting the network with frequent security upgrades and new security technologies such as Network Access Control (NAC) and Data Loss protection (DLP). As Figure 3.1.2 indicates below, a majority of respondents have already deployed, or plan to deploy for the first time, a broad array of security-related technologies.

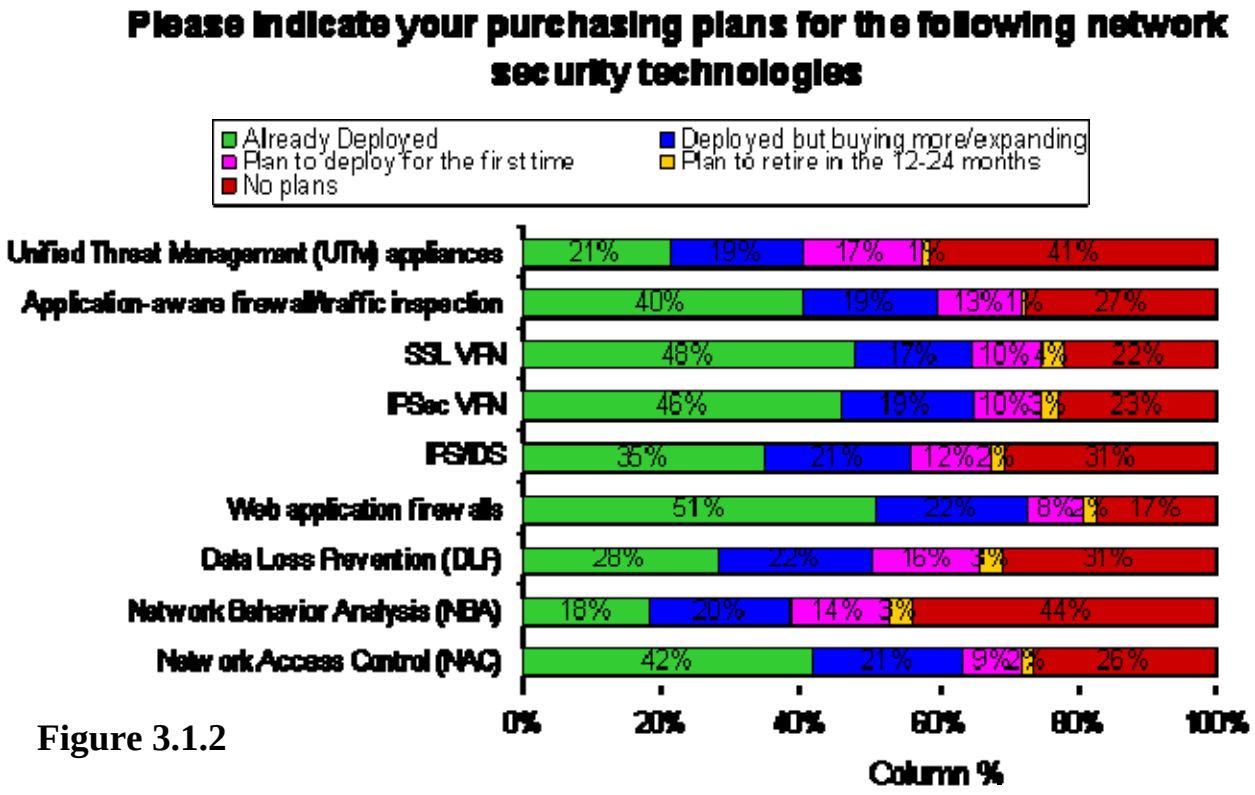

Figure 3.1.2

3.2 Gartner Group

In The Gartner Group's ("Gartner") March 31, 2008 study titled "*2008 Update: What Organizations Are Spending on IT Security*",[2] the firm describes why determining the total cost of an organization's IT security spending is difficult to do. As the study notes, few, if any, enterprises know exactly how much they spend on information security. They may be able to identify certain areas of spending for parts of the enterprise — those typically tied to the IT department — but they do not know how much they are spending across the entire enterprise on the dedicated security hardware, software, personnel and services, or how much it costs when they have to investigate and recover from a security breach.

In addition, security costs are often embedded in other areas in hidden ways because:

- IT is distributed throughout the enterprise;
- Information security is distributed — firewalls are included in the networking budget, security administration is performed by the business unit and, in many instances, these costs are not captured;

[2] See Appendix D.

- Managed security service provider (MSSP) fees are in the human resources budget since outsourcing is often considered as personnel additions;
- Enterprise security software is buried in enterprise resource planning and mainframe upgrade projects; and
- Some security safeguards can be acquired on a subscription basis, which may be classified as operations and maintenance rather than capital expenditures.

Additionally, the study indicates that Gartner considers IT security spending to be the enterprise information security costs directly related to protecting information and IT systems. This includes hardware, software, personnel, outsourcing, and consulting services associated with supporting information security across the platform, desktop and file storage environments. This also includes policies and procedures, and identity and access management. Gartner does not include physical security as an information security expense. [3]

Moreover, IT Security spending also varies depending upon the industry or sector. According to Gartner:

> *Security spending as a percentage of IT spending within the different industries is helpful in understanding the relative level of security investment of those organizations that include disaster recovery as part of IT security. Security spending is typically higher for companies that are high-visibility, in regulated environments or require higher levels of risk mitigation. This may be because of requirements for the protection of lives, financial assets, intellectual property, or of consumer, patient or student PII [personally identifiable information].*[4]

According to Gartner's January 29, 2009 study titled "*IT Spending and Staffing Report, 2009***",** the key metrics database looks at IT spending from a "cash view," in that IT spending is defined as the total of the IT operating budget (excluding depreciation and amortization), plus the planned capital expenditure (capex) for the current year.[5] In its report, Gartner provides additional detail about overall IT spend (not IT security spend) as a percentage of revenue, operating expense, as well as IT spending by employee, by region, and by industry. This data is helpful if one wants to conduct the extrapolation exercise described earlier in order to determine IT security as a percentage of overall budget, revenue, operating expense, etc.

All of the Gartner studies included as appendices provide additional detail about percentages of IT security spend by industry and geographic region, as well as how organizations prioritize and allocate their IT security investments by type of technology and security service.[6]

3.3 Forrester Group

[3] The Gartner Group, *2008 Update: What Organizations Are Spending on IT Security*, pg. 3.
[4] Ibid, pg 4.
[5] See Appendix E.
[6] See Appendices D, E, F, G, H, I & L.

The Forrester Group ("Forrester") released a study December 24, 2008 titled "*The State Of Enterprise IT Security: 2008 To 2009*" by Jonathon Penn.[7] Of the 942 participants, 42% of respondents were from companies with 1,000 to 4,999 employees; 33% were from companies with 5,000 to 19,999 employees; and 24% were from companies with 20,000 or more employees.

According to the study:

> *Security is getting a larger slice of the IT budget pie. Firms are devoting 11.7% of their company's IT operating budget to IT security in 2008 — contrasted with 7.2% in 2007 — and plan to continue nudging up IT security budgets in 2009 to 12.6% of the IT operating budget. Allocation of budget for new security initiatives mirrors this trend, going from 17.7% in 2008 to 18.5 % in 2009.*

See Figure 3.3.1, below.

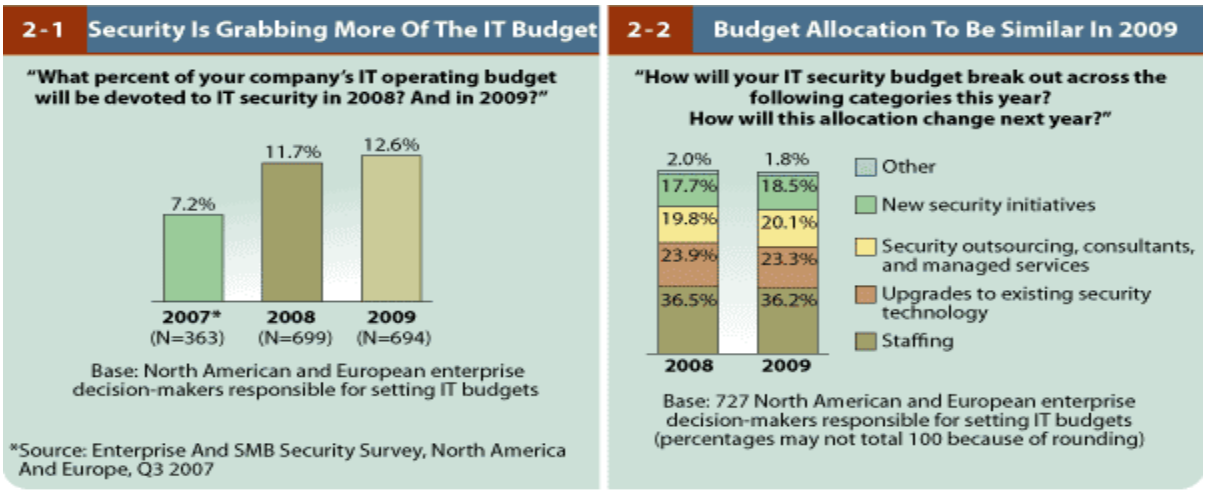

Figure 3.3.1

This document gives highlights of an extensive data set collected across North American and European enterprises via Forrester's Enterprise and Small and Medium-size Businesses (SMB) IT Security Survey, North America and Europe, Q3 2008.

During July and August 2008, Forrester fielded a survey of 2,148 North American and European IT security executives and technology decision-makers on the state of IT security. The survey explored the following areas, among others: IT security budgets; overall agenda and challenges; organizational structure; sourcing and services; policy and process; privacy; business continuity/disaster recovery; and technology adoption. When looking specifically at North American and European enterprises, the respondents indicated that IT security remains a vital aspect of the business, despite the current economic climate. For instance, the data shows that:

[7] See Appendix J.

- **IT Security budgets are increasing.** Compared with 2007, enterprises dedicated a greater percentage of their company's IT operating budget to IT security in 2008, with plans to further increase this percentage in 2009.
- **Security is increasingly reporting outside of IT.** IT security now has the attention of business executives, with more than one-third of IT decision-makers having dotted-line reporting structures to the board of executives or Chief Executive Officer.
- **Data Security is *the* top issue on the IT security agenda.** Today, security organizations are greatly concerned with protecting the company's information assets — nearly seven out of ten enterprise IT security decision-makers consider data security "very important" to the security organization.

3.4 IDC

In its response to the question raised, IDC has provided valuable qualitative data in the attached appendices on top security trends.[8] Within the report "*Worldwide IT Security Software, Hardware, and Services 2009-2012 Forecast and 2007 Vendor Shares: The Big Picture***",** IDC states that:

> *As IT budgets undergo cut backs, security spending will not be one of the areas significantly affected by this economic downturn. Increased complexity around compliance, new technologies such as virtualization and mobility, and the impact of the economic downturn will continue to fuel customer demand for security consulting and security operations services to remain competitive in a crowded marketplace and stay compliant with industry regulations.*

The IDC report appears to confirm a widely-held view that investment in security-related infrastructure and support will not be materially diminished as a consequence of an economic downturn. By all indications, the indicators demonstrate that the market for these products and services will remain strong.

[8] See Appendix K.

4.0 DIGITAL MATURITY INDEX

Question 4: Can we create an index that would measure how one country compares with another in terms of a "digital index" or a country's "digital maturity"?

A "digital index" or "digital maturity model" can serve as a useful tool for framing the discussion and approach to cyberspace and cyber security from an economic perspective, rather than solely military or national security viewpoints, as have been the lenses through which such issues are traditionally addressed. Effective technology security adoption presents a particular challenge due to the rapid development and deployment of information technologies, relative to the capacity and initiative of individuals and enterprises to safely and effectively use them. Digital maturity implies giving due consideration to society's capacity to use technology in a way that minimizes unintended and undesirable consequences.

For the purposes of this exercise, we ask the question "is there a way to capture the United States and other countries in a Digital Index which looks at the various facets of the digital age?" While indices exist for information technology (IT) industry competitiveness, research and development, and others, it would be beneficial to work with industry and academia to create an index that incorporates the unique characteristics of cyber security with those other important technology areas. The utility and value of such a Digital Index would serve to build and reinforce the case for investment in security technology development, deployment, and adoption across the IT and Communications ecosystems – from governments to industry to consumers.

The IT and Communications Sectors approached this question from two vantage points: quantitative and qualitative values necessary to develop a Digital Index to compare the United States technology and cyber security posture relative to other nations. Several indices were considered for relevance and applicability of quantitative and qualitative criteria and approaches. Examples include the Organization for Economic Co-operation and Development's *Science, Technology and Industry Scoreboard*,[9] the Economist Intelligence Unit's *IT Industry Competitiveness Index*,[10] the World Economic Forum's *Global Information Technology Report*,[11] the United Nations' *E-Government Survey*,[12] and the Democracy Index.[13] See Appendix M for additional documentation.

Any methodology should incorporate both quantitative and qualitative attributes to determine the desired data analysis. Quantitative values are typically scored from data figures and indicators

[9] Organization for Economic Co-operation and Development, *OECD Science, Technology and Industry Scoreboard 2007*, http://masetto.sourceoecd.org/vl=10526419/cl=17/nw=1/rpsv/sti2007/

[10] The Economist Intelligence Unit, *The Means to Compete: Benchmarking IT Industry Competitiveness*, http://www.bsa.org/country/Research%20and%20Statistics/~/media/12EB624EB30C486FBEA0A4B653DD5E89.ashx

[11] World Economic Forum, *Global Information Technology Report*, http://www.weforum.org/en/initiatives/gcp/Global%20Information%20Technology%20Report/index.htm

[12] United Nations E-Government Survey, http://www.zdnetasia.com/news/internet/0,39044908,62036034,00.htm

[13] Democracy Index, http://www.economist.com/markets/rankings/displaystory.cfm?story_id=8908438

that most economies assemble, and normalized via a standard formula applied across the data set. Qualitative values are usually specific to pre-determined questions and criteria that are applied to each area of focus. By combining the two types of data, derived scores and rankings could provide insight into the current state, or maturity, of the global technology and cyber security posture. However, it should be noted that to achieve any useful index, the quality and analysis of the data must be sound and reliable.

Specific quantitative indicators that would contribute to a Digital Index may include:

- Annual spending on IT infrastructure (hardware, software, and services);
- Annual spending on IT security products and services;
- Broadband penetration levels in business and consumer markets;
- Level of Internet use in the country (e.g., by number of hours spent online by users, etc.);
- Measures of societal, economic, and governmental use and dependence on the Internet and Internet-based services and applications;
- Usage of mobile communications devices;
- Level of usage of computers and the Internet in schools;
- Enrollment in higher education programs for computer science and engineering;
- Higher education programs that include cyber security as part of their curriculum;
- Employment in technology security industry;
- Prosecutions of cyber crime cases and severity of associated penalties;
- Hardware and software piracy rates;
- Investment dollars in research and development specific to cyber security;
- Applications and approvals for patents of new security technologies; and

From a qualitative perspective, there are several existing social indices such as the Democracy Index, Living Planet Index, and Human Development Index that can be used as a starting point to develop a Digital Index. Such indices are helpful for economists and others in planning and resource allocation. For example, the Democracy Index ranks countries around the world against five general categories: electoral process and pluralism, civil liberties, functioning of government, political participation, and political culture. The Democracy Index allows democratization and non-governmental organizations to direct their funds more efficiently and focus on those countries that are in greater need of democratization efforts. Similarly, a Digital Index that incorporates corresponding criteria and applies them to current technology and security conditions can provide decision-makers with valuable insights in determining which areas may need greater resources or attention.

Using the approach from the Democracy Index, the following qualitative categories are proposed for the creation of a Digital Index:

- Technology adoption effectiveness measures, such as trends in incidents, occurrences, and events involving loss above specified thresholds of personal and enterprise financial damage and disruption of operations;
- Governmental action in digitization expressed via laws, regulations, hearings, or appointments of senior officials to positions concerned with digital or cyber matters;
- Effectiveness of tools used by law enforcement agencies to detect and thwart high tech crime;

- Business implementation of digital technologies such as online banking, computerized point of sale transactions, computerized accounting and inventory management, health care records, and percentage of gross domestic product that is generated from online sales;
- Value of stock equities traded on all-electronic systems (*e.g.*, the NASDAQ conducts all transactions electronically, whereas the NYSE uses both manual and computerized trading); and
- Successful development and implementation of technology security standards.

Drawing together both quantitative and qualitative technology indicators – with an overlay of factors specific to cyber security – is an effective approach to creating a Digital Index that can provide significant insight into the current state of technology and security maturity. This data can then be used to reinforce the economic imperatives of security investment by demonstrating current and future technology trends at the macro- and micro-level. It can also serve to drive investment in certain areas that may need greater focus. It is our belief that development of such a Digital Index must be done in collaboration with industry and academia and would be a constructive and beneficial undertaking.