Cyber Security Market Trends and Government Role in Market Growth

CIVITAS
GROUP

JUNE 2009

Civitas Group llc
1110 Vermont Avenue, NW, Suite 1001
Washington, DC 20005
www.civitasgroup.com

Cyber Security Market Trends

As the density and interconnectedness of cyberspace continues to grow, so does the scale and complexity of the corresponding threat. In 2008, the United States Computer Emergency Readiness Team (US-CERT) reported 72,065 cyber-related incidents as compared to just 24,097 incidents in 2006, an increase of nearly 300% over the last two years.[i] Parallel to this trend, the computer security firm Symantec observed the rapid deployment of sophisticated tactics to overcome traditional information technology defenses deployed at the perimeter of secure networks (e.g., firewalls, intrusion detection/prevention systems). Rather than target enterprise networks through widespread, broadcast-style attacks, hackers are increasingly adopting covert strategies which compromise individual computers by exploiting trusted-site-specific vulnerabilities. In essence, hackers are using the Web itself as a conduit to distribute and execute malicious code. This technique proves increasingly difficult to detect and slow to correct, thus making it an ideal platform from which to perform a wide variety of harmful exploits. In 2008, Symantec identified 1,656,226 new malicious code threats as compared to 624,267 threats in 2007.[ii] To put that in perspective, over 60% of all known malicious code was created in the course of the last year alone.[1]

In defining the scale and complexity of the motivating threat, it becomes clear why cyber security has reasserted itself in both the public consciousness and the national priorities of government. The underlying risk, vulnerability, and cost associated with a cyber attack are continuing to increase dramatically.[iii] Within the near-future, public and private entities will attempt to reach a consensus on who has definitive ownership of this continuing problem and which solutions prove most viable in adapting the underlying architecture of the Internet to accommodate tangible gains in cyber security. The following analysis demonstrates the means by which government is increasingly exerting its authority to drive this market and the accompanying need for vendors to understand and anticipate government intervention to benefit from increased spending patterns.

Over the course of the past year, the issue of cyber security has re-emerged as a national priority and has become one of the fastest-growing segments of domestic homeland security spending. This is largely attributable to continuing public disclosures regarding the extent of information security breaches recorded in recent years – and most importantly the suspected source of those attacks, representing a significant shift from the hacker community to organized crime syndicates and state-sponsored groups. Cyber security is traditionally defined as any means of protecting information and associated information systems from unauthorized access, use, disclosure, disruption, modification, or

[1] **Note:** US-CERT defines cyber incidents as any act that violates computer security or acceptable-use policies, including: unauthorized access, denial of service, malicious code, improper usage, scans, probes, and attempted access. Symantec defines malicious code threats in terms of the number of unique signatures (including variants of existing code) that have been added to their cumulative database of potential threats. It is important to note that these two illustrative figures are not comparable metrics – the first is manually reported, the other is automatically detected (there is no direct, casual relationship between these independent statistics).

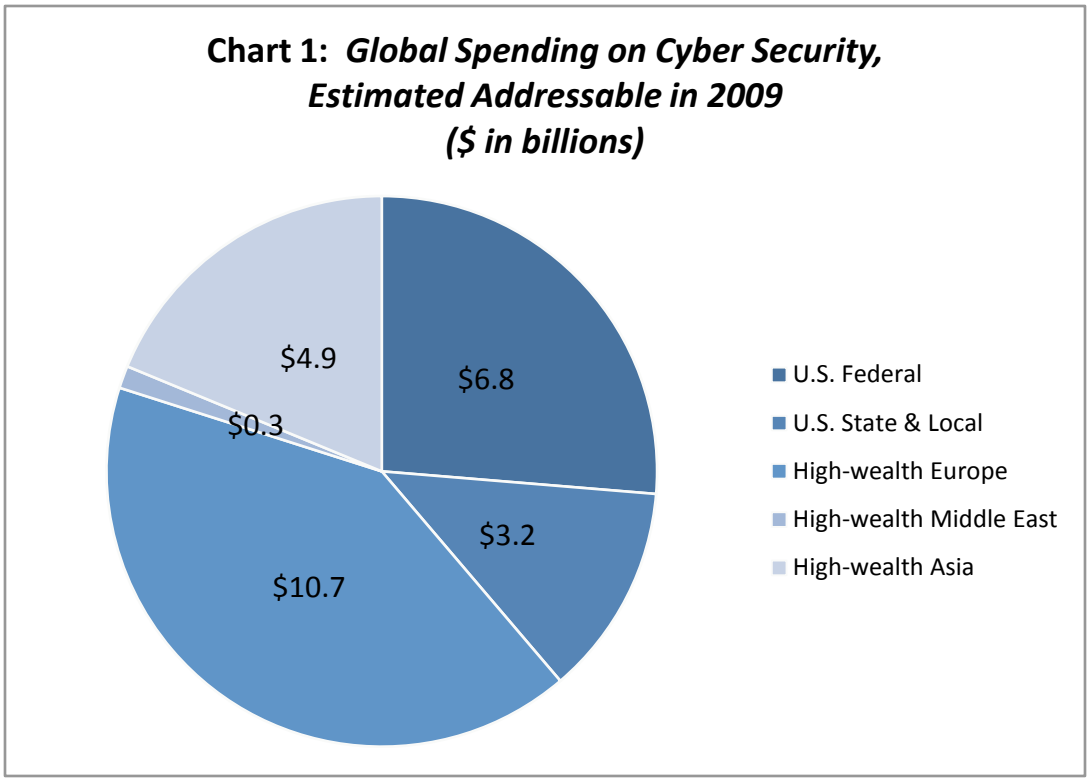
destruction.[iv] The health of our overall economy, resilience of our critical infrastructure, and integrity of our national security all remain highly dependent upon the underlying network of computers, servers, routers, switches, and fiber optic cables that constitute cyberspace.

Accordingly, we have identified five crucial market trends (depicted below) that will continue to shape the competitive landscape for cyber security products and services.

Cyber Security Market Trends

1. Due to the scale and complexity of the motivating threat, government is rapidly expanding its influence and authority over the issue of cyber security.
2. While annual growth observed in overall government IT budgets continues to flatten, IT security spending—measured in both absolute terms and as a proportion of overall IT expenditures—is experiencing continued growth.
3. Over time, the source of the underlying threat has shifted away from the autonomous hacker and towards both organized crime and state-sponsored actors. Consequently, national security concerns have become intertwined with public-private interests surrounding the protection of proprietary corporate information and intellectual property that maintain a nation's inherent competitive advantage.
4. Cyber security presents an opportunity for highly innovative solutions that move beyond passive, signature-based defensive measures and towards more sophisticated, active approaches to the emerging threat.
5. The human capital problem remains a significant obstacle in implementing comprehensive cyber security reform.

Cyber security is one of the largest homeland security mission areas, with an estimated annual spending of $25.9 billion worldwide. Of that total, the United States is the largest national market with $10.7 billion in estimated annual spending as depicted in Chart 1. It is important to note that the overall cyber security spending estimate represents only a fraction of the IT spending that governments devote specifically to IT security—it also does not include a significant portion of budgetary resources that are subject to security classification. Moreover, by all estimates, commercial investments in cyber security dwarfs this figure, and while private expenditures on cyber security products and services prove relevant to our discussion, they are not focused exclusively on responding to a homeland security mission.



Cyber Security Repurposed As National Security

The government-driven cyber security market defined above is anticipated to experience significant growth over the next five years. One catalyst was January 8, 2008 when President Bush signed dual Homeland and National Security President Directives (HSPD 23 / NSPD 54) regarding computer network monitoring and cyber security. These directives served as the primary catalyst for the Comprehensive National Cyber Security Initiative (CNCI)—a multi-agency, multi-year plan that lays out twelve areas aimed at securing the Federal government's networks.

Much of the CNCI is classified, but some information has entered the public domain. In May 2008, the Senate Armed Services Committee disclosed that the plans for CNCI called for related expenditures in excess of $17.0 billion.[v] In fact, former DHS Secretary Michael Chertoff likened the scale of the effort to that of the Manhattan Project and the House Permanent Select Committee on Intelligence characterized the CNCI as: "…the single largest request and the most important initiative of the President's fiscal year 2009 budget request."[vi,vii] Early-stage activities are expected to involve the continuing reduction of Trusted Internet Connections (TICS) into Federal agency networks and planned upgrades to DHS's passive intrusion detection system (EINSTEIN).

The impetus for the CNCI will continue to drive future market dynamics. As first articulated in the February 2003 *National Strategy to Secure Cyberspace* and reinforced since then, we

are witnessing the rapid evolution of the security threat posed by an autonomous hacker.[viii] In the past six years, we have witnessed coordinated efforts undertaken by organized crime cartels to steal personal information and perpetrate fraud online. More alarming still, we have witnessed the emergence of highly sophisticated attempts to test network defenses, penetrate secure networks, and ex-filtrate sensitive or classified data by state-sponsored actors. Hence, the nature of the underlying threat has matured from: a) petty computer crimes involving the misuse of communications equipment; to b) the illegal acquisition of personal or consumer information; to c) the theft of proprietary corporate information; and finally to d) the ability to disrupt, corrupt, or destroy vital assets in the lead-up to a conventional conflict involving kinetic weaponry. Accordingly, cyber security is being recognized as a vital means to extend the national security domain in order to protect against not only the misappropriation of the host of intellectual property that grants the United States a crucial competitive advantage, but against emerging threats.

Parallel to the activities of the CNCI, relevant government stakeholders are rapidly aligning existing organizations and laws to help implement the proposed strategy. Over the course of 2007 to 2008 alone, DHS witnessed a major reorganization of the National Cyber Security Division (NCSD) and the creation of the National Cyber Security Center (NCSC). On September 23, 2008 the Senate Homeland Security and Government Affairs Committee approved a major amendment to the Federal Information Security Management Act (FISMA), which established a new council of chief information security officers (CISOs) and requires DHS to conduct penetration tests against agency networks to identify continuing vulnerabilities.

Recently, in May 2009, the Federal Government released a 60-day comprehensive review commissioned by President Obama to assess U.S. policies and structures for cyber security. The assessment evaluates the plans, programs, and activities underway throughout the Government that address U.S. communications and information infrastructure, and offers a forward-looking framework towards a reliable, resilient, and trustworthy U.S. digital infrastructure. Together, these developments guarantee future opportunities to supplement the internal capacity of executive agencies to define departmental policies, adopt strategic planning, and implement extensive program management.

Technology and Human Capital Needs

We have identified five basic elements associated with a holistic security vision across all components of a network (segmentation depicted below). These five elements represent a diverse range of products and services. Moreover, while the cyber security market has traditionally been dominated by a discrete set of industry players (e.g., Symantec, McAfee, Trend Micro), trends indicate a real potential for emerging solutions to challenge pre-existing market dynamics. A major obstacle to implementing effective cyber security remains the simple fact that current defensive strategies encompass largely passive, signature-based approaches that remain ineffective against the rapid development of malicious code distributed discreetly.

Components of Cyber Security

1. Vulnerability and Risk Assessment
    a. Compliance, Auditing, & Reporting
    b. Network Threat Simulation
2. Network Monitoring
    a. Intrusion Detection / Prevention Systems
    b. Network Flow Analysis / Deep Packet Inspection
3. Managed Security Services
    a. Infrastructure Protection and Attack Mitigation
    b. Situational Awareness / Visualization
    c. Remote Authentication / Encryption
    d. Secure Hosting and Co-location
4. Endpoint Protection Platforms
    a. Anti-Virus / Personal Firewall
    b. "Live" Digital Forensics
    c. Virtualization / Sandboxing
    d. Software Assurance
    e. Insider Threat / Behavioral Heuristics
5. Consulting Services
    a. Policy, Planning, and Program Management
    b. Training, Education, and Awareness

This has led to a wave of innovative solutions that adopt a fundamentally new approach to emerging threats in cyberspace. In the last few years, companies have pioneered advances in deep packet inspection that allow network administrators to examine both the header and data portion of packet traffic at a pre-determined inspection point, before forwarding potentially dangerous material to its ultimate destination, thus effectively filtering risk away from the end-user. Automating this process and the associated response is a key component of the CNCI. Other companies have further adapted virtualization technology to segregate (a.k.a. "sandbox") browser-based activity from core system operations, thus effectively isolating and neutralizing known and unknown malicious code alike. Lastly, companies have begun specializing in advanced software assurance and memory forensics that search out minute changes to the operating system caused by rootkits and other malicious code that easily bypass traditional anti-virus and anti-spyware defenses. This trend towards more sophisticated, active approaches to the underlying problem represents a prime opportunity for other innovative solutions providers to fill an acknowledged gap between the current array of antiquated defenses and the rapidly accelerating nature of emerging threats.

We must acknowledge that while technology remains a critical focus of future investment, much of the work remains analytical in nature and cannot be automated. Unfortunately, there are simply not enough people with the right combination of requisite skills and security clearances to implement the vision for cyber security proposed by the CNCI. Therefore, for the foreseeable future, there remains a remarkable opportunity for firms of all sizes to form specialized work groups of qualified personnel and outsource their labor to those agencies immediately responsible for coordinating and implementing the activities of the CNCI. There is a less urgent, but equally attractive opportunity to develop a mechanism to funnel prime candidates with the right blend of education and experience into a growth segment of defense contractors' current workforce and offer a mix of career incentives that government cannot presently guarantee.

Finally, we note that much of the architecture of the CNCI presumes a successful scale-up of extant capabilities developed and deployed to protect far smaller subnets (e.g. the .ic domain). While such an effort is justified by the urgency of the threat, the issue of whether the architecture and its associated technologies are up to the challenge remains problematic. Hence, providers in this area should be alert to the shortcomings of the current plan, and position themselves to step in with innovative solutions or even alternative architectures should problems arise.

Conclusion

In summary, the cyber security mission area is best characterized by a set of five reinforcing market trends. First, the scale and complexity of the motivating threat has reached a point which has led government to expand its influence and authority over the issue of cyber security. Understanding and anticipating the nature of government intervention will prove vital to those firms seeking to benefit from increased spending patterns. Second, while annual growth in general government IT spending continues to flatten under increased pressure to demonstrate cost effectiveness, IT security spending continues to grow rapidly—this set of inverse trends is likely to persist for the foreseeable future. Third, over time, the source of the underlying threat has shifted from the autonomous hacker to organized crime and state-sponsored actors. Consequently, national security concerns have become intertwined with public-private interests surrounding the protection of proprietary corporate information and intellectual property that maintain the nation's inherent competitive advantage. Fourth, cyber security presents the opportunity for highly innovative solutions that move beyond passive, signature-based defensive measures and towards more sophisticated, active approaches to emerging threat. Fifth, a significant gap in implementing comprehensive cyber security reform is the human capital element—there are simply not enough analytical personnel with the right combination of requisite skills and security clearance to execute the current strategy. We believe that an investor's ability to anticipate these trends in advance and adapt accordingly will largely determine his relative level of success in accessing the cyber security market.

About the Authors:

The Civitas Group provides strategic advisory and investment services for those operating in the homeland and national security arena. Civitas has a successful history of supplying subject matter expertise to Federal, state, local, and select international governments, providing objective analyses of their operations and activities, and enabling proactive policy development and informed decision making. Civitas has a proven track record of working with the private sector—Fortune 100 firms, global technology providers, early stage companies with promising technologies, and private investment firms—to grow their businesses, find partners and capital, and build service and technology platforms.

References

[i] Ben Bain, "Number of Reported Cyber Incidents Jumps," *Federal Computer Week*, February 17, 2009. http://fcw.com/Articles/2009/02/17/CERT-cyber-incidents.aspx.

[ii] Symantec Enterprise Security, *Global Internet Security Threat Report, Trends for 2007*, Volume XIV, Published April 2009, Page 10, http://www.symantec.com/business/theme.jsp?themeid=threatreport.

[iii] Government Accountability Office, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats (07-705)*, June 2007, Table 4: Economic Impact of Cybercrime, http://www.gao.gov/new.items/d07705.pdf.

[iv] 44 USC § 3542 (b)(1), *Public Printing and Documents, Coordination of Federal Policy, Information Security, Definitions,* http://www.law.cornell.edu/uscode/html/uscode44/usc_sec_44_00003542----000-.html.

[v] Senate Committee on Armed Services Report (110-335), *National Defense Authorization Act for FY2009*, 110th Congress, 2nd Session, http://thomas.loc.gov/cgi-bin/cpquery/T?&report=sr335&dbname=110&.

[vi] Remarks by Homeland Security Secretary Michael Chertoff to the 2008 RSA Conference, San Francisco, April 8, 2008, http://www.dhs.gov/xnews/speeches/sp_1208285512376.shtm.

[vii] House Permanent Select Committee on Intelligence Report (110-665), *Intelligence Authorization Act for FY2009*, 110th Congress, 2nd Session, http://www.fas.org/irp/congress/2008_rpt/hrpt110-665.html.

[viii] White House, *National Strategy to Secure Cyberspace*, February, 2003, http://www.whitehouse.gov/pcipb/.