GAO
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-13-187, a report to congressional addressees

Why GAO Did This Study

Cyber attacks could have a potentially devastating impact on the nation's computer systems and networks, disrupting the operations of government and businesses and the lives of private individuals. Increasingly sophisticated cyber threats have underscored the need to manage and bolster the cybersecurity of key government systems as well as the nation's critical infrastructure. GAO has designated federal information security as a government-wide high-risk area since 1997, and in 2003 expanded it to include cyber critical infrastructure. GAO has issued numerous reports since that time making recommendations to address weaknesses in federal information security programs as well as efforts to improve critical infrastructure protection. Over that same period, the executive branch has issued strategy documents that have outlined a variety of approaches for dealing with persistent cybersecurity issues.

GAO's objectives were to (1) identify challenges faced by the federal government in addressing a strategic approach to cybersecurity, and (2) determine the extent to which the national cybersecurity strategy adheres to desirable characteristics for such a strategy. To address these objectives, GAO analyzed previous reports and updated information obtained from officials at federal agencies with key cybersecurity responsibilities. GAO also obtained the views of experts in information technology management and cybersecurity and conducted a survey of chief information officers at major federal agencies.

View GAO-13-187. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

February 2013

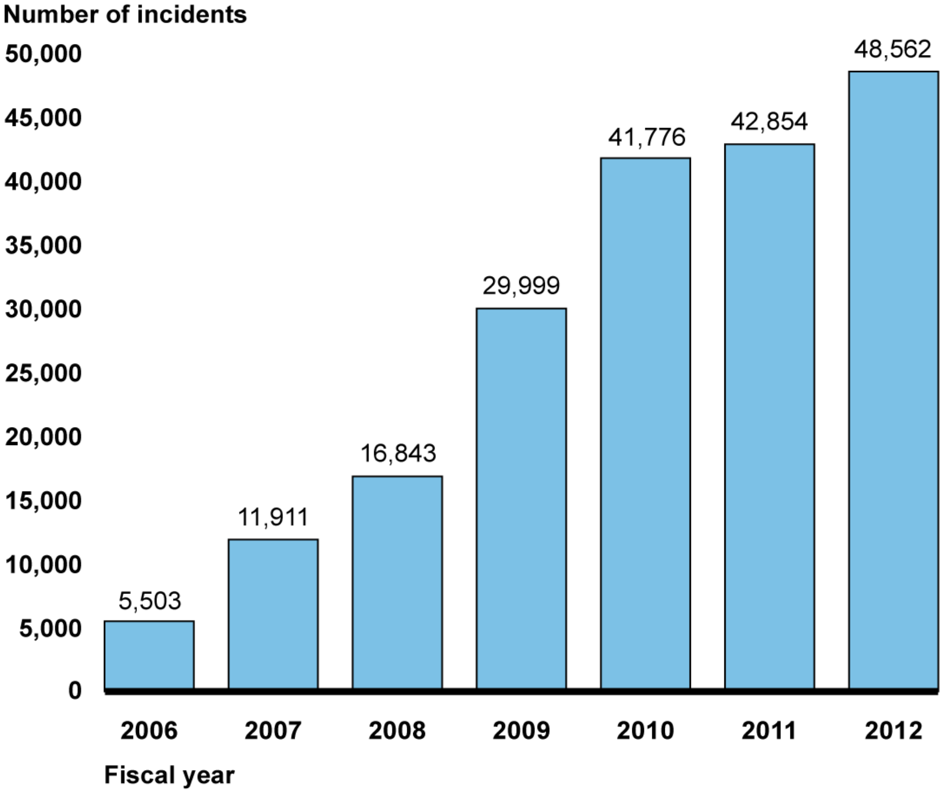
CYBERSECURITY

National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented

What GAO Found

Threats to systems supporting critical infrastructure and federal operations are evolving and growing. Federal agencies have reported increasing numbers of cybersecurity incidents that have placed sensitive information at risk, with potentially serious impacts on federal and military operations; critical infrastructure; and the confidentiality, integrity, and availability of sensitive government, private sector, and personal information. The increasing risks are demonstrated by the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, and steady advances in the sophistication and effectiveness of attack technology. As shown in the figure below, the number of incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team has increased 782 percent from 2006 to 2012.

Incidents Reported by Federal Agencies in Fiscal Years 2006-2012



Source: GAO analysis of US-CERT data for fiscal years 2006-2012.

GAO and inspector general reports have identified a number of key challenge areas in the federal government's approach to cybersecurity, including those related to protecting the nation's critical infrastructure. While actions have been taken to address aspects of these, issues remain in each of these challenge areas, including:

- **Designing and implementing risk-based federal and critical infrastructure programs.** Shortcomings persist in assessing risks, developing and implementing controls, and monitoring results in both the federal government and critical infrastructure. For example, in the federal arena, 8 of 22 major agencies reported compliance with risk management requirements under the Federal Information Security Management Act (FISMA), down from 13 out of 24 the year before. In the critical infrastructure arena, the Department of Homeland Security (DHS) and the other sector-specific agencies have not yet identified cybersecurity guidance applicable to or widely used in each of the critical sectors. GAO has continued to make numerous recommendations to address weaknesses in risk management processes at individual federal agencies and to further efforts by sector-specific agencies to enhance critical infrastructure protection.
- **Detecting, responding to, and mitigating cyber incidents**. DHS has made incremental progress in coordinating the federal response to cyber incidents, but challenges remain in sharing information among federal agencies and key private sector entities, including critical infrastructure owners, as well as in developing a timely analysis and warning capability. Difficulties in sharing and accessing classified information and the lack of a centralized information-sharing system continue to hinder progress. According to DHS, a secure environment for sharing cybersecurity information, at all classification levels, is not expected to be fully operational until fiscal year 2018. Further, although DHS has taken steps to establish timely analysis and warning, GAO previously reported that the department had yet to establish a predictive analysis capability and recommended that DHS expand capabilities to investigate incidents. According to the department, tools for predictive analysis are to be tested in fiscal year 2013.
- **Promoting education, awareness, and workforce planning**. In November 2011, GAO reported that agencies leading strategic planning efforts for education and awareness, including Commerce, the Office of Management and Budget (OMB), the Office of Personnel Management, and DHS, had not developed details on how they were going to achieve planned outcomes and that the specific tasks and responsibilities were unclear. GAO recommended, among other things, that the key federal agencies involved in the initiative collaborate to clarify responsibilities and processes for planning and monitoring their activities. GAO also reported that only 2 of 8 agencies it reviewed developed cyber workforce plans and only 3 of the 8 agencies had a department-wide training program for their cybersecurity workforce. GAO recommended that these agencies take a number of steps to improve agency and government-wide cybersecurity workforce efforts. The agencies generally agreed with the recommendations.
- **Promoting research and development (R&D)**. The goal of supporting targeted cyber R&D has been impeded by implementation challenges among federal agencies. In June 2010, GAO reported that R&D initiatives were hindered by limited sharing of detailed information about ongoing research, including the lack of a repository to track R&D projects and funding, as required by law. GAO recommended that a mechanism be established for tracking ongoing and completed federal cybersecurity R&D projects and associated funding, and that this mechanism be utilized to develop an ongoing process to make federal R&D information available to federal agencies and the private sector. However, as of September 2012, this mechanism had not yet been fully developed.
- **Addressing international cybersecurity challenges**. While progress has been made in identifying the importance of international cooperation and assigning roles and responsibilities related to it, the government's approach to addressing international aspects of cybersecurity has not yet been completely defined and implemented. GAO recommended in July 2010 that the government develop an international strategy that specified outcome-oriented performance metrics and timeframes for completing activities. While an international strategy for cyberspace has been developed, it does not fully specify outcome-oriented performance metrics or timeframes for completing activities.

The government has issued a variety of strategy-related documents over the last decade, many of which address aspects of the above challenge areas. The documents address priorities for enhancing cybersecurity within the federal government as well as for encouraging improvements in the cybersecurity of critical infrastructure within the private sector. However, no overarching cybersecurity strategy has been developed that articulates priority actions, assigns responsibilities for performing them, and sets timeframes for their completion. In 2004, GAO developed a set of desirable characteristics that can enhance the usefulness of national strategies in allocating resources, defining policies, and helping to ensure accountability. Existing cybersecurity strategy documents have included selected elements of these desirable characteristics, such as setting goals and subordinate objectives, but have generally lacked other key elements. The missing elements include:

- **Milestones and performance measures**. The government's strategy documents include few milestones or performance measures, making it difficult to track progress in accomplishing stated goals and objectives. The lack of milestones and performance measures at the strategic level is mirrored in similar shortcomings within key government programs that are part of the government-wide strategy. The DHS inspector general, for example, recommended in 2011 that DHS develop and implement performance measures to be used to track and evaluate the effectiveness of actions defined in its strategic implementation plan. As of January 2012, DHS had not yet developed the performance measures but planned to do so.

- **Cost and resources**. While past strategy documents linked certain activities to budget submissions, none have fully addressed cost and resources, including justifying the required investment, which is critical to gaining support for implementation. In addition, none provided full assessments of anticipated costs and how resources might be allocated to address them.
- **Roles and responsibilities**. Cybersecurity strategy documents have assigned high-level roles and responsibilities but have left important details unclear. Several GAO reports have likewise demonstrated that the roles and responsibilities of key agencies charged with protecting the nation’s cyber assets are inadequately defined. For example, the chartering directives for several offices within the Department of Defense assign overlapping roles and responsibilities for preparing for and responding to domestic cyber incidents. In an October 2012 report, GAO recommended that the department update its guidance on preparing for and responding to domestic cyber incidents to include a description of its roles and responsibilities. In addition, it is unclear how OMB and DHS are to share oversight of individual departments and agencies. While the law gives OMB responsibility for oversight of federal government information security, OMB transferred several of its oversight responsibilities to DHS. Both DHS and OMB have issued annual FISMA reporting instructions to agencies, which could create confusion among agency officials because the instructions vary in content. Clarifying oversight responsibilities is a topic that could be effectively addressed through legislation.
- **Linkage with other key strategy documents**. Existing cybersecurity strategy documents vary in terms of priorities and structure, and do not specify how they link to or supersede other documents, nor do they describe how they fit into an overarching national cybersecurity strategy. For example, in 2012, the administration determined that trusted Internet connections, continuous monitoring, and strong authentication should be cross-agency priorities, but no explanation was given as to how these three relate to priorities previously established in other strategy documents.

The many continuing cybersecurity challenges faced by the government highlight the need for a clearly defined oversight process to ensure agencies are held accountable for implementing effective information security programs. Further, until an overarching national cybersecurity strategy is developed that addresses all key elements of desirable characteristics, overall progress in achieving the government's objectives is likely to remain limited.

What GAO Recommends

To address missing elements in the national cybersecurity strategy, such as milestones and performance measures, cost and resources, roles and responsibilities, and linkage with other key strategy documents, GAO recommends that the White House Cybersecurity Coordinator develop an overarching federal cybersecurity strategy that includes all key elements of the desirable characteristics of a national strategy. Such a strategy would provide a more effective framework for implementing cybersecurity activities and better ensure that such activities will lead to progress in cybersecurity.

This strategy should also better ensure that federal departments and agencies are held accountable for making significant improvements in cybersecurity challenge areas, including designing and implementing risk-based programs; detecting, responding to, and mitigating cyber incidents; promoting education, awareness, and workforce planning; promoting R&D; and addressing international cybersecurity challenges. To address these issues, the strategy should (1) clarify how OMB will oversee agency implementation of requirements for effective risk management processes and (2) establish a roadmap for making significant improvements in cybersecurity challenge areas where previous recommendations have not been fully addressed.

Further, to address ambiguities in roles and responsibilities that have resulted from recent executive branch actions, GAO believes Congress should consider legislation to better define roles and responsibilities for implementing and overseeing federal information security programs and for protecting the nation’s critical cyber assets.

In its comments, the Executive Office of the President agreed that more needs to be done to develop a coherent and comprehensive strategy on cybersecurity but did not believe producing another strategy document would be beneficial. However, GAO believes an overarching strategy document that includes milestones and performance measures, cost and resources, roles and responsibilities, and linkage with other key strategy documents would provide a more effective framework for implementing cybersecurity activities. The Executive Office of the President also agreed that Congress should consider enhanced cybersecurity legislation.