Written Testimony
U.S. House of Representatives
Permanent Select Committee on Intelligence
Arthur W. Coviello, Jr.
Executive Chairman, RSA, The Security Division of EMC
October 4, 2011

Chairman Rogers, Ranking Member Ruppersberger, and other distinguished Members of the Committee, thank you for the opportunity to testify today about cyber security threats to our nation.

My name is Art Coviello. I am an Executive Vice President at EMC Corporation and Executive Chairman of RSA, The Security Division of EMC. RSA provides security, compliance and risk management solutions for organizations worldwide. RSA helps the world's leading organizations succeed by solving their most complex and sensitive security challenges so they can safely benefit from the tremendous cost and productivity gains of digital technology and the Internet. EMC Corporation is a global leader in enabling businesses and third-party providers to transform their operations and deliver IT as a service. Fundamental to this transformation is cloud computing. Through innovative products and services, EMC accelerates the journey to cloud computing, helping IT departments store, manage, protect and analyze their most valuable asset – information – in a more agile, trusted and cost-efficient way.

The U.S., like many other nations, is highly dependent upon information technology in everything from national security and intelligence activities, to commerce and business, to personal communications and social networking. The Internet is one of the unifying fabrics driving globalization and political change at an increasingly accelerated pace. Information technology (IT) is vital to every major industry and economy in the world. Simply put, these technologies and associated network communications systems represent the greatest opportunity to enhance our productivity and to spread our system of values. Unfortunately, due to the dynamic nature of today's IT environments, these evolving technologies and modes of communication also represent one of our greatest threats. Therefore, it is not surprising that cyber security has become such an important economic and national security issue.

Today's hearing topic also is one that hits close to home for our company. From our vantage point as a provider of security solutions, we are seeing the rapid evolution of the threat landscape, with more varied targets, and in many cases, more advanced technologies and tactics than ever before. This expansion in risk is threatening to erode trust in the digital commerce, communication and collaboration that we all take for granted today. Recently, we gained first-hand experience in the sophistication and determination of today's cyber adversaries.

As you know, RSA publicly disclosed on March 17, 2011, that we had detected a targeted cyber attack on our systems and that certain information related to the RSA SecurID® product had been extracted. We immediately developed and published best practices and remediation steps, and proactively reached out to thousands of customers across the public and private sectors to help them implement those steps. Further, we worked with the appropriate U.S. federal government agencies and several information sharing and analysis centers (ISACs) to ensure broad communication of these best practices and remediation steps as well as information about the attack.

The attack on RSA reflects the sophistication of today's attackers in understanding the interconnections and interdependencies that organizations have in our networked world and how to exploit our inter-dependence to achieve their goals. In other words, we are seeing increases in attacks on one organization to be leveraged in an attack on another organization. It was a stark reminder for us – and for the entire community of information security practitioners – that no organization that embraces the Internet and information technology, whether public or private, is immune to cyber attacks.

According to the 2011 Data Breaches Investigation Report by Verizon, in 86 percent of breaches studied, the victim was notified of the breach by a third party, such as law enforcement, a customer or a partner, after the breach had occurred.[1] Fortunately, we were able to discover the attack on RSA in progress, which allowed us to quickly disclose it to our customers including the remediation advice and options. We regret the incident and apologize for the inconvenience and anxiety the attack caused our customers. To date, we know of only one instance where it has been indicated that information stolen from us was a factor in the attack on another organization, and that organization reported that the attack was unsuccessful.

The attacks on RSA and others have become a valuable lesson that has redoubled our motivation to lead a call-to-action to increase industry understanding of today's advanced threats while also collaborating with a broader community of stakeholders to better prepare for and mitigate advanced cyber attacks.

Across the range of cyber adversaries it is clear that the preferred method of exploitation centers on people. Social engineering is now the number one avenue of attack, and the new security perimeter is the human being because related attacks easily evade traditional perimeter controls such as anti-virus software, firewalls and intrusion detection systems. Security professionals have long understood that IT users will click on links they shouldn't and unwittingly install malware hidden through simple ruses. Corporate IT departments deploy multiple controls to help deal with this threat. This process may work well for generic attacks, but not for sophisticated zero-day exploits. Consequently, because there is no way to prevent all people associated with organizations from making mistakes, organizations need to assume compromise is probable if not inevitable if they are to defend themselves thoroughly.

---

[1] 2011 Data Breaches Investigation Report, Verizon, 2011

However, the increased probability of a hostile presence on a network does not mean that an organization's valuable information inevitably will be stolen, altered or misused. There are steps that industry and government can take to detect and disrupt attacks and create more agile defenses that will help deter attackers and protect the "crown jewels" of information that are within our organizations. Some of these steps require technology, some require reinvigorating risk management processes, some depend on the creation of more effective ecosystems of technology partners, some require additional investments in education and training, and still others require changes in government policy.

Before I address steps that can help organizations better manage cyber risks, it is important to have a discussion and understanding of the ways in which IT and the threat landscape are evolving.

Understanding the Scope of the Cyber Threat

In the past 15 years, we've had an explosion of information, with it being created at an ever increasing rate and spreading further and faster than ever before. Along with this growth has been a flood of productivity-enhancing web applications and personal-computing devices. Every one of us is both consuming new technologies from devices like iPads and Droid-based smartphones to social networks like LinkedIn and Facebook and trying to deal with their unprecedented entry into our organizations. Are organizations ceding more control of their IT environments to their users? Yes. Will transitioning to cloud computing make it easier or harder to protect our sensitive digital information? That will depend on how it is implemented.

The Internet and all of its facets permeate every corner of our organizations and personal lives. Our situation is complicated and especially challenged by what I call "degrees of openness." The number of parties with whom we do transactions and share information is skyrocketing and the velocity of those transactions and information sharing is increasing. The hyperextension of our enterprises and the wonders of more ubiquitous and simple online access are introducing new complexities, new vulnerabilities and new opportunities for the darker elements of the Internet. The attackers are exploiting those vulnerabilities – easily outflanking perimeter defenses.

To successfully defend against these attacks it is important to better understand the actors. The attackers can be categorized into three major classes of cyber adversaries: criminals, non-state actors, and nation states each with distinct motives and modus operandi but who may, at times, collaborate if their goals align.

Criminals

One class is the cyber criminal. Whether loosely affiliated or tightly organized, they are out to steal information assets that can be converted to cash. It's typical to see their "platform-based" crimeware and zero-day vulnerabilities auctioned on the black market to the highest bidder. A criminal group can buy a botnet kit for drive-bys, a spamming kit for spam runs, bulletproof hosting from an underground service provider,

un-attributable domain registration, and on and on. As the criminal ecosystem matures, the cost of entry for cyber crime continues to fall.

Non-state Actors

This category of actors is made up of those who have a non-sovereign agenda and who are investing disproportionately with respect to any returns they might see. The category includes publicity seeking hackers (or so called "hacktivists") with political agendas. They are the ones who want to send you a very loud message and broadcast it to members of the media. Whether it is Web vulnerabilities, lack of general security controls, or the failure of the human firewall, these groups will find the holes in an organization's mythical security perimeter. They can be very sophisticated online hackers themselves or can work with or encourage insiders with access to important information.

This category also includes terrorists. With tools such as Stuxnet, now more available and accessible, the possibility of terrorists obtaining malware like this is increasing. In the future, their agendas could include combined physical attacks with cyber attacks on critical infrastructure.

Nation States

A third category of attacker is the nation state. Nation states typically are focused on: gaining strategic advantage through theft of government secrets and valuable intellectual property; ensuring competitive advantage for their domestic industries; or gaining intelligence on their own citizens or those of other nations who they believe present a risk to them. They also have the ability to combine physical attacks with cyber attacks on infrastructure.

Nation-sponsored attacks are often the most sophisticated and are carried out with stealth. The attack may start like any other – simple and under the radar with rudimentary malware and a variety of tools no different from the other groups. The real differences in sophistication are the concentration of resources behind the attack and efficiency with which these adversaries operate after gaining entry. They almost always do a lot of intelligence gathering – sometimes for months – in advance of the attack. They know which end users in corporations or government agencies possess the assets they want through social media and other means. They develop a solid mapping and inventory of the target network and security infrastructure over time. Experience tells them where the information they want resides (in critical databases, or file shares, for example). They almost always start with client-side attacks, with malware embedded in Flash files or PDF documents, including custom backdoors and rootkits. Advanced threats tend to incorporate malware produced hours or days before the attacks, so that traditional anti-virus tools have no signature by which to identify or block it. They compromise a directory of users, obtain access to local service accounts or take over domain administrator accounts.

Finally, they are also difficult to detect because very often they have compromised one company to be used in attacking another. Unlike cyber criminals, they want to remain inside an organization's network, so they go quiet, set up backup systems,

and monitor incident response efforts to gauge defender responses, and alter their behavior accordingly.

Adjusting Risk Management and Technology Strategies

With that review of the threat landscape, let's take a look at what can be done to address these challenges.

The new fact of life for IT organizations is a state of persistent, dynamic, intelligent threat and disruption. The security dogmas of the past are no longer adequate. Many security technologies in common use across U.S. public and private enterprises are past their freshness date, offering diminished value in a world of advanced threats.

Security must evolve from conventional frameworks of an uncoordinated lineup of static point products to more advanced security systems capable of meeting more dynamic threats and agile enough to meet the advanced challenges of the hyper-extended enterprise. Instead, organizations need to be more flexible and develop and maintain security programs, processes, and technologies that can evolve ahead of – or at least alongside – the threat landscape. An advanced security system designed to defend against advanced threats should be risk-based, agile and contextual, not relying on static or update dependent controls against "known bad" threats. Let me spend some time addressing the characteristics of an advanced system.

Risk-based

Risk is a function of the vulnerabilities inherent in today's open IT infrastructures, the probability of being attacked and the materiality of the consequences. All organizations must have a clear and prioritized inventory of all information assets and their relative value to the organization, its stakeholders, and mission objectives. Against this information inventory, you must understand the discrete security exposure of these assets, which is a complex equation that combines elements of technology strengths and vulnerabilities, the maturity of your business and IT processes, and the awareness and commitment of your people. Evaluating the true risk of your information assets from the point of various classes of adversaries enables you to gain a sense of the relative risks, likelihood of attack and success, and the potential level of effort needed to manage risk. All of this work requires a lot of information and many sources of business and security intelligence.

So, how do you execute and manage this risk-management approach throughout your entire enterprise? To execute and manage this process, organizations need to deploy an advanced governance, risk and compliance (GRC) framework to manage policies, controls, risks and assessments and make this information available to key mission owners. An advanced GRC framework allows organizations to respond quickly to new threats, address program deficiencies and reduce vulnerabilities across all domains and lines of business**,** but only if the system of controls operating within the framework is up to the challenge.

Agile

Many existing controls lack the situational awareness, visibility and agility needed to detect and thwart sophisticated attacks. Controls that have these capabilities today – DLP, adaptive authentication, claims-based access control and controls embedded in virtual environments, need to be deployed within organizations more pervasively. These controls can be better leveraged if they are combined with advanced and continuous monitoring technologies in a systemic way, creating a modernized vision for defense-in-depth.

The threat landscape will continue to evolve, and a successful outcome requires that organizations have the agility to process, incorporate and analyze new sources of internal and external intelligence on the fly. Automation is absolutely essential for security to work at the speed and scale of the networks and cyber threats we face. In the near future, an advanced security system will rely on predictive analytics based on an understanding of normal states, user behaviors, and transaction patterns to spot high-risk events and allow organizations to proactively adapt defenses.

Agile defense also requires that the people and the technology must become smarter with each incident. Security activities should yield a net increase in capabilities and intelligence, versus a rediscovery of something already known by others. Eventually, organizations will adopt "intelligent automation" to simplify security management processes and handle mundane remediation and intelligence creation tasks without human intervention.

Contextual

This advanced system of controls can only be effective when a security event is delivered with complete context around it. In other words, the success of prioritization and decision making is dependent on having the best information available. Advanced security systems need to rely on more than just traditional security event management and correlation tools. Organizations must adopt a "big data" view of information security from which their security teams have real-time access to the entirety of information relevant to the detection of security problems.

From a security perspective, big data refers to vast data sets of unprecedented scale and formats – gathered from every part of the enterprise – all requiring correlation through real-time analysis and the ability to act on insights in automated ways. The use of big data is enabled by advances in data storage systems and computing power and analytics that, when combined, eliminate the trade-off between the cost to collect and store data and the cost and time required to analyze the data. The security industry now has the technology that fuses high-speed analytics with security intelligence and large volumes of network and systems data, giving organizations the contextual view needed to defend against advanced threats. And, as organizations continue to transition to cloud infrastructure and services, we believe that these "big data" capabilities will become more common and more critical in security.

I believe virtually everything we do in IT will transition to the cloud over the next 10 years as organizations continue to move business and IT functions that are not core competencies to cloud providers who can do them better and more cost effectively. At EMC, we also see this transition to cloud computing as an opportunity to improve information security. Cloud computing, which is fundamentally changing the way organizations think about and implement IT, can enable organizations to improve their information security by replacing the disparate and piecemeal legacy IT systems that are so common today. Cloud computing enables IT and information security organizations to implement centralized monitoring, management, compliance, and security solutions. In addition, security is being built into the information infrastructure that makes up the foundation for cloud computing including virtualization and data storage platforms.

In this era of tight budgets and rapidly evolving threats, government should look to industry to provide the bulk of advanced security technologies to the government. When considering the development and deployment of advanced technologies, the government should leverage commercially developed solutions that have a proven track record across a broad threat landscape.

Developing More Effective Ecosystems

Even with better risk management processes and as organizations continue to move away from perimeter-based defenses, our community must develop security ecosystems that will be an integral part of a comprehensive advanced defense strategy. A robust and dynamic public-private partnership will need to be at the center of this effort.

Just as our cyber adversaries create their own ecosystems, we must improve information sharing within the industry and with our partners in government, both in the U.S. and abroad. Beyond the open source and proprietary resources out there today, we all must be committed to create more robust opportunities for information exchange that include the private sector, ISACs, and government agencies alike. The more actionable and real-time information sharing that we have, the better chance we have in keeping pace with cyber adversaries rather than simply reacting after they strike.

Automated cyber intelligence information sharing – the ability for organizations to share threats and incidents at machine speed – is a critical need for defending our cyber infrastructure. As the attacks on our cyber infrastructure increase in breadth and sophistication, the urgency to address this challenge continues to grow. Today, there are many government and commercial groups that strive to share threat and incident information, but their approaches are limited and manual-intensive. Current approaches are inadequate to handle the complexity and volume of the threat information, and because they are primarily manual, they have difficulty keeping up with the real-time nature of the threat.

We cannot change the game in information sharing if we do not start thinking differently and expand beyond traditional approaches. In the private sector, we have to be willing to work with competitors and continue to build trusted relationships within and across vertical industries, but we also need to develop improved technical mechanisms to

share information in real-time. Continued development of processes to ensure the anonymity among competitors will also help. But concerns about liability when sharing sensitive information present significant constraint. It is incumbent on government to help address those concerns. I will discuss this more later when making some specific policy recommendations, but concerns over liability will need to be addressed to build more effective ecosystems.

Government has to think differently as well about how it is sharing its information with the private sector. When information is shared between private sector organizations and government agencies, the tendency to over-classify that information (even when the attack happens on a commercial network) and/or to make it law-enforcement-sensitive, creates real obstacles to productive two-way information exchange. In addition, multiple agencies with different missions and types of legal agreements create additional challenges to actionable two-way information sharing between government and industry.

The public sector should further leverage information available from commercial services to give a fuller picture of the threat landscape. For example, the RSA Anti-Fraud Command Center (AFCC) has worked globally with financial institutions, ISPs, law enforcement and other organizations to detect and shut down hundreds of thousands of phishing attacks. We also have worked with industry-led ISACs that are partnering with government entities and law enforcement – such as the Financial Services ISAC[2] – to provide timely and actionable information on cyber threats and attacks. Actionable information gained from these mechanisms and in other processes with industry is often as valuable as information from government sources.

We also need better collaboration between industry and government across all areas of cyber security, and several organizations are working on this issue. At the national level, the Enduring Security Framework is a partnership of senior industry and government executives to identify critical cyber vulnerabilities and mobilize experts to address the risks. At the regional level, the New England Advanced Cyber Security Center is a consortium of industry, government, and universities working together to share cyber threats and explore new areas of research required to improve our defenses. EMC and RSA are active in both of those initiatives, and we believe progress is being made in a number of areas.

Given the substantial attention that the U.S. Congress has paid to supply chain security issues, we also think that there should be a better understanding of industry-led efforts in that area. First, there are a range of issues that are often lumped into the "supply chain" bucket, ranging from worries about counterfeit products ending up in national security systems to foreign influence on the integrity of software and hardware developmental processes. I would encourage Members of this Committee to review two

[2]For more information on the FS-ISAC's information sharing practices and programs, see "Testimony of William B. Nelson, The Financial Services Information Sharing & Analysis Center" before the U.S. House of Representatives Financial Institutions and Consumer Credit Subcommittee, September 14, 2011.

short white papers[3] published in 2009 and 2010 by the Software Assurance Forum for Excellence in Code (SAFECode) that provides clarity about issues around software integrity in the supply chain. SAFECode (www.safecode.org), a non-profit organization that EMC co-founded, is dedicated to increasing trust in technology products and services through the advancement of effective software assurance methods.[4]

EMC also joined other leading IT vendors and services companies along with several U.S. federal agencies in the formation of the Open Group Trusted Technology Forum (O-TTF), a global forum established to promote the adoption of best practices, such as secure engineering and supply chain integrity processes that can be adopted by technology providers and their suppliers. Building on an earlier white paper[5] that the group published outlining their framework, O-TTF is working to create a global supply chain protection standard early next year along with the capability to accredit organizations that formally adopt the practices. The group is also actively working with standards entities like NIST and Common Criteria to align this new work to create synergy as they move forward. We encourage this Committee to be briefed on the Forum's initiatives and encourage NIST to further align with these industry efforts.

Another public-private partnership model that we can build upon is the National Cyber Security Alliance or NCSA (www.staysafeonline.org), a non-profit organization. The Alliance, comprised of captains of industry from sectors ranging from the defense sector and IT industry to financial services and e-commerce providers to telecommunications and ISPs, has been working with government at all levels on a national user awareness education campaign. Our company has been involved in this partnership for several years and as the cyber security challenge has grown, so has the Alliance.

In collaboration with its public-sector partners, NCSA established *National Cyber Security Month* in October, which is designed to elevate and expand cyber security awareness programs that the President of the United States and the U.S. Congress have promoted and endorsed via resolutions and other activities. The U.S. Department of Homeland Security (DHS) is a long-time participant and supporter of this public-private partnership as are multiple other federal government agencies and many state and local governments. NCSA, working with the Anti-Phishing Working Group (APWG) and DHS, launched the Stop-Think-Connect awareness campaign, an effort that could be expanded into a Smokey-the-Bear-like nationwide initiative with help from Congress and the Administration.

---

[3] "The Software Supply Chain Integrity Framework: Defining Risks and Responsibilities for Securing Software in the Global Supply Chain", SAFECode, July 21, 2009.

[4] Also see "Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain", SAFECode, June 14, 2010.

[5] "Open Trusted Technology Provider Framework: Industry Best Practices for Manufacturing Technology Products that Facilitate Customer Technology Acquisition Risk Management Practices and Options for Promoting Industry Adoption", The Open Group Trusted Technology Forum, February 2011.

Education and Training

Even as we develop stronger ecosystems, we also need to keep an eye on the future by investing in education and training. Both public and private sector organizations are unable to fill thousands of cyber security positions, simply because they lack qualified candidates. As cyber threats escalate at an alarming rate, we need to invest in building the cyber security workforce with the requisite skills to defend our enterprises, government and critical infrastructure and help drive continued innovation. Two areas of investment are particularly important.

Cyber security programs in our post-secondary schools: Our colleges and universities must produce graduates with the technical and cross-functional skills needed to defend against our cyber adversaries. To defend our networks, we will need to graduate more individuals with expertise in computer sciences, risk assessment, data mining, data visualization and analytics, digital forensics, and human behavior. The federal government should support programs at the college and university levels that graduate qualified cyber security professionals. Successful government-funded scholarship programs, such as the National Science Foundation, DHS, and NSA funded Scholarship for Service programs that have produced many highly qualified cyber professionals now working in both the public and private sectors should be expanded.

Training, certification and accreditation programs to increase and maintain cyber security proficiency: Government and private enterprises should provide various levels of training opportunities for their IT staff starting with traditional organizations that offer security certifications such as The SANS Institute and the International Information System Security Certification Consortium (ISC2) and Information Systems Audit and Control Association (ISACA) that provide education and certification programs.

But we need to go farther than we have in the past. A number of organizations and industry leaders believe that specific sectors require periodic accreditation of security professionals in certain job classes. The recently formed National Board of Information Security Examiners (www.NBISE.com) shows great promise as an accreditation authority for our industry that can improve the performance of our cyber security workforce. Through its programs and research, NBISE helps to validate hands-on skills and knowledge in order to reliably predict an individual's future performance and aptitude for cyber security. The government also should examine the benefits of requiring re-certification and accreditation within its training programs.

There are other important initiatives currently underway in the area of education. Bodies such as National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce should continue to provide forums for best practices, frameworks for standards, and as a key dissemination point for relevant information. In addition, new programs such as the U.S. Cyber Challenge are being put into place to identify, recruit and place the next generation of cyber security professionals.[6]

[6] For more information, go to the U.S. Cyber Challenge Website at: http://workforce.cisecurity.org/

Updates to Government Policy

Because cyber security has become a critical national and economic security issue, government clearly has a crucial role to play and should act to make needed updates to government policy.

With advanced cyber security threats gaining so much attention, resulting in substantial information loss and significant harm in many cases, it is hard to argue that our national government should not act now. But what can be achieved through legislation that could make a positive difference while minimizing the possible unintended consequences of new laws? And, since American businesses – large and small – operate in a global economy, how can policies be crafted to enhance U.S. technology competitiveness, so that innovation will not be slowed and growth in international markets not deterred?

As this Committee and the U.S. House of Representatives consider federal cyber security legislation, we encourage you to focus on outcomes rather than prescribing technologies or checklist-heavy compliance programs. There also are legislative steps that Congress can take now that we believe could help advance cyber security in both the public and private sectors, and there are areas where we think Congress should be very cautious about instituting legislative action.

1. Be cautious about addressing global supply chain challenges with legislation

While there are legitimate concerns about supply chain security, the problem should not be over-stated. And if the Administration or Congress adopts policies for the U.S. that are very restrictive, other governments are watching these developments closely and could take actions that will further restrict entry of U.S.-based companies in their home markets. Prescriptive mandates in this area could undermine U.S. economic competiveness and also fail to address specific challenges for securing global IT supply chains.

It is EMC's belief that if the U.S. is to move forward effectively to improve our defense-in-depth capability across global interconnected supply chains, we must build on common sense security practices that are scalable as we deliver effective technology solutions. The focus should be on rationalizing and streamlining overlapping acquisition policies that often prevent or delay the government's ability to leverage the most advanced security products. We recommend leveraging the work of private-public partnerships such as the O-TFF and SAFECode, while developing policies and mapping to global industry standards and best practices. In short, we encourage Congressional oversight of this area, but we do not recommend new legislative requirements.

2. Update U.S. laws and penalties to account for cyber-crimes and build stronger cooperation with other countries to deter cyber attacks

The Administration's proposal to clarify several existing criminal offenses related to attacks on computers and computer networks would be a good start. Congress should

also build on the Administration's International Strategy for Cyberspace.[7] In addition, Congress should consider approaches such as the *International Cyber-crime Reporting and Cooperation Act* – bipartisan legislation that could empower the U.S. government to better utilize several levers to address cyber crime internationally, including foreign assistance and trade agreements.

3. Encourage public-private information sharing by addressing liability concerns

This past July in Washington, DC, RSA and TechAmerica (www.techamerica.org) brought together leading security experts from the public and private sectors to discuss defense strategies against advanced persistent threats. One of the key areas that participants zeroed in on was barriers that impede effective information exchange. Fear of legal risks topped the list of the biggest impediments to sharing actionable threat information. This is an area that Congress could address now. One approach is to provide a safe harbor or similar protections for organizations that voluntarily share sensitive threat information with the government and/or the information sharing and analysis centers (ISACs). Such an approach could help improve situational awareness and cyber readiness for many organizations while reducing serious concerns about legal risk.

4. Enact a federal data breach notification law to reduce complexity and provide regulatory relief

Congress should act now to reduce the regulatory complexity that businesses and critical infrastructure organizations have to deal with complying with myriad state data breach disclosure laws. While we believe the first-in-the-nation California data breach law enacted nearly a decade ago, was the right approach as it prompted organizations to better manage risks to personally identifiable information (PII), the time has come for a federal law that will replace the 46 disparate state breach notification laws.

In an advanced threat environment, it does not make sense to have organizations devoting their resources and focus to complying with 46 separate state laws on breach notification when they need to invest more time and resources in managing operational cyber security risks. Simplifying the compliance requirements with a reasonable and uniform federal standard (with preemption of the existing state laws) would allow security organizations to focus more on risk management.

5. Spur the adoption of an effective risk management framework for critical infrastructure – but don't overreach with regulation

There has been much discussion about how to best protect critical infrastructure from cyber threats and how to spur the adoption of effective risk management processes and controls in those organizations. We encourage Congress to work with industry to, as necessary, create an updated framework for covered critical infrastructure organizations

[7] The President's International National Strategy for Cyberspace was released in May 2011

to: 1) conduct a risk assessment, and 2) based on that risk assessment, put effective risk management processes and practices in place.

There should be a timetable set for these assessments, and the federal government should also have an ability to verify that the covered critical infrastructure organizations have completed their risk assessments and addressed the risks discovered during that process. We believe that the National Infrastructure Protection Plan offers a baseline framework to build on.

Congress should not prescribe what practices should be put in place based on risk assessments – an organization should have the flexibility to match controls and best practices that are based on global industry standards. One possible model for this approach is the current guidance from the Federal Financial Institutions Examination Council (FFIEC) guidance for *Authentication in an Internet Banking Environment*.[8] The guidance focuses on an outcome, is technology neutral and requires that organizations conduct a risk assessment and then put controls in place that are appropriate and commensurate with the identified risk.

6. Update the Federal Information Security and Management Act

Security must be risk-based and driven by flexible policy that is aligned to both the changing threat landscape and the business or mission need. The need for a common framework to ensure that security policies are consistently applied across the infrastructure is critical to success. However, this framework should allow Federal agencies to focus their audit function on addressing their system vulnerabilities and weaknesses based on the attacks that are exploiting them, not a 25-year-old manual of general security controls. Enabling continuous monitoring is essential to address today's threat environment and provide an effective operational risk management framework for tomorrow's cloud computing infrastructure. These are two of the principal reasons EMC supports updating the Federal Information Security and Management Act (FISMA). The Office of Management and Budget (OMB) has issued important guidance that established continuous monitoring requirements and Cyberscope. The General Services Administration (GSA) and NIST have also developed FEDRAMP, which provides a standard approach to accessing and authorizing cloud computing services and products for use by federal agencies.

These are six practical policy recommendations that we think could assist organizations as risk managers and security organizations grapple with advanced cyber threats. The U.S. Congress can help improve our nation's cyber security posture now by: acting to update criminal laws and penalties; reducing liability concerns; eliminating the regulatory complexity that organizations face today by enacting a federal data breach law; working with the private sector to update as needed the risk management framework for covered critical infrastructure; modernizing FISMA; and coming up with reasonable

[8] The FFIEC Guidance to Authentication in an Internet Banking Environment was issued in October 2005 and supplemented guidance was issued in June 2011. http://www.ffiec.gov/press/pr062811.htm

and effective policy approaches to supply chain protection that will not stifle innovation and competitiveness.

# # #

Thank you for the opportunity to testify in front of this Committee today. I would be happy to answer questions you may have at this time.