Prepared Testimony and
Statement for the Record of

Dean Turner
Director, Global Intelligence Network
Symantec Corporation

Hearing on

Cybersecurity: Assessing the Immediate Threat to the United States

Before the

U.S. House of Representatives
Committee on Oversight and Government Reform
Subcommittee on National Security, Homeland Defense and Foreign Operations

May 25, 2011

2154 Rayburn House Office Building

INTRODUCTION

Chairman Chaffetz, Ranking Member Tierney, and Members of the Subcommittee, thank you for the opportunity to appear before you today as the Committee considers cybersecurity and the current threat to the United States.

My name is Dean Turner and I am the Director of the Global Intelligence Network at Symantec Corporation. My primary responsibilities include designing and delivering our security intelligence data feeds and developing next generation security intelligence toolsets that provide greater visibility into the threat landscape. I have co-authored and managed Symantec's Internet Security Threat Report which is a trusted source of global research and analysis on cyber attack data gathered from the Global Intelligence Network.

Symantec[1] is the world's information security leader with over 25 years of experience in developing Internet security technology. Today we protect more people and businesses from more online threats than anyone in the world. Our best-in-class Global Intelligence Network allows us to capture worldwide security intelligence data that gives our analysts an unparalleled view of the entire Internet threat landscape including emerging cyber attack trends, malicious code activity, phishing and spam. We maintain eleven Security Response Centers globally and utilize over 240,000 attack sensors in more than 200 countries to track malicious activity 24 hours a day, 365 days a year. In short, if there is a class of threat on the Internet, Symantec knows about it.

In 2010, Symantec security technology blocked more than three billion attacks on individual and enterprise systems. In addition, we saw the threat landscape become exponentially more hazardous, with the discovery of 14 new zero-day vulnerabilities, 163 new mobile vulnerabilities, 6,253 new vulnerabilities, and 286 million new unique variants of malicious code. As an example of the magnitude of the threat, in the time it takes to read this testimony, Symantec will block more than 365,000 attacks against our customers.

At Symantec, we are committed to assuring the security, availability, and integrity of our customers' information. The protection of critical infrastructure is a top priority for us. We believe that critical infrastructure protection is an essential element of a resilient and secure nation. From water systems to computer networks, power grids to cellular phone towers, risks to critical infrastructure can result from a complex combination of threats and hazards, including terrorist attacks, accidents, and natural disasters.

Symantec welcomes the opportunity to provide comments as the Committee continues its important efforts to ensure that adequate policies and procedures are in place, both in the private sector and in the federal government, to monitor and secure critical systems from cyber attack. In my testimony today, I will provide the Committee with:

- Symantec's latest analysis of the evolving threat landscape as detailed in the *Symantec Internet Security Threat Report Volume XVI (ISTR XVI)*;
- An assessment of the real-world impacts of cyber attacks on business and individuals;
- Insights into the major challenges and vulnerabilities associated with securing new technologies; and
- Observations on how organizations can better secure these systems.

[1] Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

EVOLVING THREAT LANDSCAPE

In April 2011, we published the latest *Symantec Internet Security Threat Report Volume XVI (ISTR XVI)*[2], where we observed significant changes to the threat landscape that existed in 2010. The volume and sophistication of threat activity increased substantially, with Symantec identifying more than 286 million new threats last year.

However, to understand the evolving threat landscape, we first should understand who is behind the vast array of cyber attacks that we are seeing today. Attacks originate from a range of individuals and organizations, with a wide variety of motivations and intended consequences. Attackers can include hackers (both individual and organized gangs), cybercriminals (from petty operators to organized syndicates), cyber spies (industrial and nation state), and "hacktivists" (with a specific political or social agenda). Consequences can also take many forms: from stealing resources and information, to extorting money, to outright destruction of information systems.

It is also important to recognize that attackers have no boundaries when it comes to who their intended victims are. All organizations and individuals are potential targets of those who seek to do harm. Corporate enterprises are often the object of targeted attacks specifically to steal customer data and intellectual property, but also to disrupt business processes and commerce. Small businesses are often less resilient and the impacts of stolen bank accounts and business disruption can be catastrophic in a very short time frame. End-users or consumers are confronted with the financial and disruptive impacts of identity theft, scams, and system clean-ups, not to mention the lost productivity and frustration of restoring their accounts. Finally, governments are most often the victims of cyber sabotage, cyber espionage, and hactivism, that can have significant national security implications.

To develop the ISTR, Symantec analyzes data from the malicious code intelligence it gathers from more than 133 million client, server, and gateway systems that have deployed our antivirus products. Additionally, Symantec's distributed "honeypot" network collects data from around the globe, capturing previously unseen threats and attacks that provide valuable insight into attacker methods. We also maintain one of the world's most comprehensive vulnerability databases, currently consisting of more than 40,000 recorded vulnerabilities (spanning more than two decades) affecting more than 105,000 technologies from more than 14,000 vendors.

Spam and phishing data are captured through a variety of sources, including the Symantec Probe Network, a system of more than 5 million decoy accounts, MessageLabs™ Intelligence, a respected source of data and analysis for messaging security issues, trends and statistics, as well as other Symantec technologies. Data is collected in more than 86 countries around the globe. Over 8 billion email messages, as well as over 1 billion Web requests are processed per day across 16 data centers. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors, and more than 50 million consumers.

These resources give Symantec's analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The result is the Symantec ISTR XVI, in which we observed five key threat landscape trends in 2010.

1. Targeted attacks continue to evolve

The year 2010 was book-ended by two significant targeted attacks, including Hydraq (a.k.a. Aurora) and Stuxnet. While there were some major differences observed in these attacks such as scale, motivations and

[2] *Symantec Internet Security Threat Report XVI, April 2011*. http://www.symantec.com/business/threatreport/index.jsp

backgrounds of alleged attackers, they had one thing in common – their victims were specifically targeted and compromised, even though many had implemented security measures.

Stuxnet was a game changer, exemplifying just how sophisticated and targeted threats are becoming. It demonstrated the vulnerability of critical national infrastructure industrial control systems to attack through widely used computer programs and technology. Stuxnet also served as a wake-up call to critical infrastructure owners and operators around the world. It was the first publicly known threat to target industrial control systems and grant hackers vital control of critical infrastructures such as power plants, dams and chemical facilities.

Another type of targeted attack is known as "spear-phishing." While the high-profile, targeted attacks that received a high degree of media attention such as Stuxnet and Hydraq attempted to steal intellectual property or cause physical damage on a major scale, spear-phishing attacks simply prey on individuals for their personal information. In 2010, for example, data breaches caused by hacking resulted in an average of over 260,000 identities exposed per breach—far more than any other cause. Breaches such as these can be especially damaging for enterprises because they may contain sensitive data on customers as well as employees that even an average attacker can sell on the underground economy.

2. Hide and seek (zero-day vulnerabilities and rootkits)

Though not always necessary to carry out effective targeted attacks, zero-day vulnerabilities often play a role. A zero-day vulnerability is one for which there is sufficient public evidence to indicate the vulnerability has been exploited in the wild prior to being publicly known. In 2010, Symantec observed 14 new zero-day vulnerabilities, an increase from 12 in 2009. Stuxnet is a notorious example, as it used an unprecedented four of these zero-day vulnerabilities. Of course, all vulnerabilities can pose a risk. Symantec documented a total of 6,253 new vulnerabilities in 2010, a 30 percent increase over 2009 and more than in any previous reporting period. The number of new vendors affected by vulnerabilities also increased to 1,914, a 161 percent increase over 2009.

Attackers also leveraged rootkits to evade detection, allowing the threat to remain running on a compromised computer longer, and thereby increasing the potential harm it can do. A rootkit is a collection of tools that allow an attacker to hide traces of a computer compromise from the operating system and, by extension, the user. They use hooks into the operating system to prevent files and processes from being displayed and prevent events from being logged. For example, if a Trojan (malicious software programs that masquerade as benign applications or files), or a backdoor is detected on a computer, the victim may take steps to limit the damage, such as changing online banking passwords and canceling credit cards. However, if the threat goes undetected for an extended period, this not only increases the possibility of theft of confidential information, it also gives the attacker more time to capitalize on this information.

3. Social networking + social engineering = compromise

Social networks continue to be a security concern for organizations, as government agencies and companies struggle to find a satisfactory compromise between leveraging the advantages of social networking, and limiting the dangers posed by the increased exposure of potentially sensitive and exploitable information. Malicious code that uses social networking sites to propagate remains a significant concern. Dumpster diving for paper-based personally identifiable information has now given way to the riches of social networking sites where individuals and organizations readily post their most sensitive information.

Attackers can gather other information from social networking sites that can indirectly be used in attacks on an enterprise. For example, an employee may post details about changes to the company's internal software or hardware profile that may give an attacker insight into which technologies to target in an attack. All it takes is a single negligent user or unpatched computer in the employee's list of friends to give attackers a beachhead into the organization from which to mount additional attacks on the enterprise -- from within, often using the credentials of the compromised employee.

Another one of the chief concerns is the popularity of shortened URLs. Attackers are increasingly using shortened URLs because they can obscure the actual destination of the link from the user. Potential victims are unable to quickly determine where the URL will send them, leaving them more vulnerable to a phishing scam or malware infection. A favorite method used to spread an attack from a compromised social networking profile is to post links to malicious websites from that profile, so that the links appear in the news feeds of the victim's friends. During a three-month period in 2010, nearly two-thirds of malicious links in news feeds observed by Symantec used shortened URLs.

As more people join social networking sites and the sophistication of these sites grows, it is likely that increasingly complex attacks will be perpetrated through them. Users should ensure that they monitor the security settings of their profiles on these sites as often as possible, especially because many settings are automatically set to share extensive, potentially exploitable information.

4. Attack kits get a caffeine boost

While targeted attacks are focused on compromising specific organizations or individuals, attack toolkits attempt to exploit anyone unfortunate enough to visit a compromised website. In 2010, attack toolkits continued to see widespread use with the addition of new tactics. A typical toolkit today is built to allow the criminal to monetize infected machines in every way possible. Not only can it record everything a user types on a system (keystroke loggers are a simple way to capture any password a user types in), but it can also steal email addresses found on the machine (to sell to spammers or to attack other users) and add additional malware to the machine at any time (remote access allows the criminal to download and execute any file they want).

Web attack toolkits are similar to "off the shelf" products that automatically create obfuscated html code containing exploits. They are user-interface driven and can even collect stats on how many users have been infected by their "product." The organized nature of attack toolkits and their ability to self update over the Web, greatly increase the speed at which new vulnerabilities are exploited and spread.

One of the most significant attack kits , known as the Zeus Trojan, is a favorite of cybercriminals, due to its ease of use and low cost (about $400) in the underground economy. It takes little to no technical knowledge to launch this attack, and it can be extremely profitable for cybercriminals. Several gangs using Zeus have been charged with theft in the millions of dollars.

We are also seeing an increase in the prevalence of "shot gun attacks," whereby web attack kits make it easy to blast many different attack vectors at once. Today it is not unusual to see single attacks that target tens - if not hundreds - of different weaknesses in a user's defenses, increasing the chances for success.

Globally, the number of Web-based attacks per day increased by 93 percent in 2010 compared to 2009. Since two-thirds of all Web-based threat activity observed by Symantec is directly attributed to attack kits, these kits are likely responsible for a large part of this increase.

5. Mobile threats increase

As more users download and install third-party applications for mobile devices, the opportunity for installing malicious applications is also increasing. Most malicious codes now are designed to generate revenue. Hence, there will likely be more threats created for these devices as people increasingly use them for sensitive transactions such as online shopping and banking. Trojans that steal data from mobile devices, and phishing attacks, will likely be some of the first of these threats to arrive.

In a sign that the mobile space is starting to garner more attention from both security researchers and cybercriminals globally, there was a 42 percent increase in the number of reported new mobile operating system vulnerabilities, from 115 in 2009 to 163 in 2010.

Currently, the majority of malicious code for mobile devices is in the form of Trojans that pose as legitimate applications. These applications are uploaded to mobile application marketplaces where users download and install them. In some cases, attackers may take a popular legitimate application and add additional code to it. On the horizon, we also are seeing proofs of concept for stealing information off mobile memory cards and the running of botnets on mobile devices.

REAL-WORLD IMPACTS

Symantec has conducted a number of recent studies and surveys to look more closely at the real-world impacts that today's cyber threats have on critical infrastructures, corporate enterprises, small businesses and consumers. A number of these findings are highlighted below.

- **Norton Cybercrime Report 2010: Human Impact**

In 2010, Norton, the consumer division of Symantec, conducted a groundbreaking global study exposing the alarming extent of cybercrime and the feelings of powerlessness and lack of justice felt by its victims. The *Norton Cybercrime Report 2010: Human Impact* [3] study included more than 7,000 adults from 14 countries.

The study revealed that 65 percent of adults worldwide report being a victim of cybercrime, and most of those surveyed expect to be scammed or defrauded online at some point, with less than one in 10 people saying they feel 'very' safe online. In addition, 79 percent do not expect cybercriminals to be brought to justice, indicating a growing prevalence of fear and trepidation associated with Internet usage, along with a general theme of powerlessness. Further, the study showed that most victims take an average of 28 days, at an average cost of $334 to resolve a cybercrime attack.

- **Symantec Consumerization of IT from the End User's Perspective Survey**

The *Symantec Consumerization of IT from the End User's Perspective Survey* [4] revealed that the number of employee-owned endpoints is growing. The growing uptake of smartphones and tablets, and their increasing connectivity and capability, has resulted in a rise in the number of users downloading and installing third-party applications for these devices. This in turn increases users' security risk exposure of installing malicious applications. In fact, the same study revealed that 52 percent of respondents felt that employee-owned endpoints somewhat compromise security and increase data loss threats. While employers are

[3] *Norton Cybercrime Report 2010: Human Impact.* www.norton.com/cybercrimereport
[4] *Symantec Consumerization of IT from the End User's Perspective Survey, May 2011.* http://www.symantec.com/connect/blogs/survey-results-consumerization-it-end-user-s-perspective-2

communicating mobile device security policies and/or best practices, they are primarily dealing with the loss or theft of devices, with malicious apps still taking a backseat, leaving the employer's and the employee's information vulnerable.

Companies must not underestimate the impact of data breach as a result of the consumerization of IT and mobility of employees. This creates security gaps in business processes, increasing the likelihood and extent of data loss threats. Accordingly, there is an urgent need for companies to address these issues and take action to reduce the level of security and data loss risks to which they are exposed. Enterprises need to understand what and how endpoints are being used in their organizations, identify where and how their sensitive data is being stored and accessed, and establish criteria and data security policies to manage, govern and enforce compliance across the corporation.

- **Symantec 2011 Small & Mid-sized Business Disaster Preparedness Survey**

The global threat landscape underscores the need for small and mid-sized businesses (SMBs) to evaluate their current security policies to ensure they are prepared for today's risks. In January 2011, Symantec released the *Small and Mid-sized Business Disaster Preparedness Survey*[5] in which we found that SMBs are still not taking disaster preparedness seriously when it comes to their IT systems. Half of the SMBs we surveyed said they do not have a plan, 52 percent do not think that computer systems are critical to their business, and 40 percent say data protection is not a priority.

According to the study, 65 percent live in areas prone to disasters, and in the past year, SMBs experienced an average of six IT outages. If SMBs aren't prepared for that risk, the impact of a potential disaster, whether natural or manmade, can be expensive. An IT outage costs SMBs an average of $12,500 per day if their computers are down, not including its effect on their customers (which averaged $10,000 per day). In fact, 54 percent of SMB customers switched SMB vendors due to unreliable computing systems, and 29 percent of customers indicated that they lost "some" or "a lot" of important data such as credit card information, patient records, or other financial information.

- **Symantec 2010 Critical Infrastructure Protection Survey**

Our nation's critical information infrastructure is characterized as including businesses and industries whose importance is such that if their cyber networks were successfully breached and disabled, it could result in a threat to national security. The vast majority of the nation's critical infrastructure is owned and operated by the private sector. In August 2010, Symantec commissioned a Critical Infrastructure Protection (CIP) Survey to assess the level of attacks against and the readiness of owners and operators. The survey included 1,580 enterprises in 15 countries worldwide, with companies ranging from 10 employees to more than 10,000. The median company size was between 1,000 and 2,499 employees. We focused on six key critical infrastructure segments: Energy, Banking and Finance, Communications, Information Technology, Healthcare, and Emergency Services.

We discovered that the threat of such attacks is real and organizations will continue to be at risk of being targeted by specific attacks. *Symantec's 2010 CIP Survey*[6] included the following highlights:

---

[5] *Symantec Small & Mid-sized Business Disaster Preparedness Survey*, January 2011. http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=dpsurvey&om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Jan_worldwide_dpsurvey

[6] *Symantec Critical Infrastructure Protection Survey*, September 2010. http://www.symantec.com/content/en/us/about/presskits/Symantec_2010_CIP_Study_Global_Data.pdf

- Critical infrastructure providers are being attacked. Fifty-three percent of companies suspected experiencing an attack waged with a specific goal in mind. Of those hit, the typical company reported being attacked 10 times in the past five years. Forty-eight percent expect attacks in the next year and 80 percent believe the frequency of such attacks is increasing.

- Attacks are effective and costly. Respondents estimated that three in five attacks were somewhat to extremely effective. The average cost of these attacks was $850,000.

- Industry is willing to partner with government on CIP. Nearly all of the companies (90 percent) said they have engaged with their government's CIP program, with 56 percent being significantly or completely engaged. In addition, two-thirds have positive attitudes about programs and are somewhat to completely willing to cooperate with their government on CIP.

- Room for readiness improvement. Only one-third of critical infrastructure providers feel extremely prepared against all types of attacks and 31 percent felt less than somewhat prepared. Respondents cited security training, awareness and comprehension of threats by executive management, endpoint security measures, security response, and security audits as the safeguards that needed the most improvement.

NEW TECHNOLOGIES = NEW RISKS & REWARDS

Virtualization and cloud computing promise the next wave of technological evolution in the way we manage desktops as well as data centers. However, with rapid adoption of new technologies come new risks. As highlighted in the Symantec ISTR XVI, the increased use and relative simplicity and effectiveness of attack kits has contributed to their increased use in cybercrimes — these kits are now being used in the majority of malicious Internet attacks. This new trend has attracted traditional criminals who would otherwise lack the technical expertise in cybercrime, fuelling a self-sustaining, profitable, and increasingly organized global underground economy. Cybercriminals who are financially motivated are now able to easily launch malware anytime and anywhere, stealing confidential information such as customer credit card information or intellectual property, from enterprises or end-users. Existing technological solutions suggest that detection capability of these targeted attacks would be a lot more effective on the cloud than on the desktop.

With 80 percent of respondents globally planning to use cloud computing much more intensively two years from now, (according to a survey conducted by the Ponemon Institute for Symantec[7]), the cloud's growing popularity will increase the risk of being targeted by cybercriminals. However, despite widespread interest and benefits in adopting cloud computing technologies, many organizations are still 'flying blind' with respect to making them secure, potentially putting their business operations, company data and customer information at risk. Most organizations lack the procedures, policies and tools to ensure that sensitive information they put in the cloud remains secure. In fact, the same study revealed that only 27 percent of respondents said their organizations have procedures for approving cloud applications that use sensitive or confidential information.

[7] Ponemon Institute, *Flying Blind in the Cloud: The State of Information Governance*, April 2010. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-ponemon_institute_flying_blind_in_the_cloud_WP.en-us.pdf

These findings indicate the need for IT managers to be more involved in the deployment of cloud computing services within their organizations. At Symantec, we believe the success of the cloud computing model hinges on the level of trust and confidence between service providers and service consumers. Vendors and service providers that can successfully address the security, compliance and privacy challenges will be the winners in the era of cloud computing.

If cloud security is appropriately implemented, there is an array of benefits to be gained, from efficiency to improved and more rapid protections. Security benefits include:

- Increased visibility because it is possible to more easily identify attacks and suspicious behavior where data from multiple sources is aggregated together.
- Scaling advantages as large cloud providers can invest in sophisticated monitoring and dedicated security personnel that are shared across a customer base where any single customer may not be able justify the cost. The same advantages exist for a cloud provider investing in multiple data centers and connectivity for redundancy.
- Should an issue be detected in a cloud environment that affects one single customer, the issue can be fixed once and the protection is shared across the entire customer base, even if they are not (yet) exposed to the new threat.
- The existence of a cloud layer provides for an additional layer of defense, thereby increasing the strategic depth of the defender and the layers of security that the attacker needs to successfully penetrate.

However, over and above providing hosted security services, it is critical for organizations to view and manage their security environment in a holistic manner – both on-premises and in the cloud. Interoperability between on-premise security tools and cloud-based tools is critical. These entities must work together to maximize the security benefits that they both bring.

To ensure the security and success of cloud computing, Symantec sees the critical need for security to evolve in the following areas:

- Ensure that policies and procedures clearly state the importance of protecting sensitive information stored in the cloud. The policy should outline what information is considered sensitive and proprietary.
- Organizations should adopt an information governance approach that includes tools and procedures for classifying their information and understanding risk so that policies can be put in place that specify which cloud-based services and applications are appropriate and which are not.
- Evaluate the security posture of third parties before sharing confidential or sensitive information. As part of the process, corporate IT and/or information security experts should conduct a thorough review and audit of the vendor's security qualifications.
- Prior to deploying cloud technology, organizations should formally train employees on how to mitigate the security risks specific to the new technology to make sure sensitive and confidential information is protected.

In other words, when discussing threat protection, especially technological threats, one needs to remember that the world is changing rapidly, therefore the technology and security has to keep up. The strive for security is very much a moving target and we must continue to stay ahead of the curve to protect our data and our networks.

PROTECTING NETWORKS AGAINST THREATS & PREVENTING DATA LOSS

Deployment and management of an anti-malware solution is the first step in network protection. But this solution alone does not provision the entire security landscape. You must also be constantly watching out for and monitoring vendor security notifications and alerts, and apply needed patches or workarounds as soon as possible. Ensuring that users are kept up to date through a security education and awareness program is vital to keeping networks secure. Last, but not least, know your assets, identify your perimeter of secure operations, and maintain a high level of situational awareness to ensure you are aware of, and can respond to, incidents in a timely manner for the sake of operational survival.

In light of the current key threat trends, and recent high-profile cases such as WikiLeaks and other data breaches, it has also become critical for all organizations to establish and implement a sustainable data loss prevention (DLP) program that effectively addresses evolving risk factors. A comprehensive, long-term, sustainable DLP program is based on the following principles:

- **Threat coverage:** Information must be protected wherever it resides, whether at-rest, in-motion or in-use. This requires control points at multiple tiers (i.e. endpoint, gateway, network, back-end databases). Further enhanced compatibility with a cloud environment and Web 2.0 sites provides a more transparent Web experience for end-users that seamlessly prevents data exposure.
- **Data Insight:** DLP should help enterprises identify their most critical information and enable simplified data clean-up and remediation through automated data owner identification. Besides continuous monitoring and auditing of data usage DLP needs to ensure adherence with corporate policies and regulatory compliance.
- **Business Process Integration:** DLP must be incorporated into an organization's overall business process so that it is viewed as a business necessity, aligned with strategic goals, compliance requirements and risk management.
- **Risk Reduction Measurement:** Enterprises should define achievable and measurable goals and then regularly review progress against them and hold business leaders accountable for meeting them.
- **Identify critical information and simplify remediation:** Effective DLP solutions should include a unified platform that allows customers to create policies once, and enforce them everywhere to prevent confidential data loss across endpoint, network and storage systems. Integrated DLP technology helps enterprises align their information assets to business goals by simplifying the remediation of exposed critical data.

To reduce the risk of data breaches, organizations require a clear understanding about where their sensitive data resides and how it is being used. With this insight, organizations will be better placed to identify gaps in their strategy, better equipped to define their requirements, and better prepared to implement a data governance plan that will reduce their risk posture.

ENSURING RESILIENCY AGAINST CYBER ATTACKS

We have learned many lessons from Stuxnet and other recent attacks. While the sophistication level of attacks is increasing, as is the potential and real damage caused by such attacks, we must turn these lessons into action. Symantec recommends the following steps be taken in order to better protect critical systems from cyber attack:

- **Develop and enforce IT policies** and automate compliance processes. By prioritizing risks and defining policies that span across all locations, organizations can enforce policies through built-in automation and

workflow and not only identify threats but remediate incidents as they occur or anticipate them before they happen.

- **Protect information** proactively by taking an information-centric approach. Taking a content-aware approach to protecting information is key in knowing who owns the information, where sensitive information resides, who has access, and how to protect it as it is coming in or leaving your organization. Utilize encryption to secure sensitive information and prohibit access by unauthorized individuals.
- **Authenticate identities** by leveraging solutions that allow businesses to ensure only authorized personnel have access to systems. Authentication also enables organizations to protect public facing assets by ensuring the true identity of a device, system, or application is authentic. This prevents individuals from accidentally disclosing credentials to an attack site and from attaching unauthorized devices to the infrastructure.
- **Manage systems** by implementing secure operating environments, distributing and enforcing patch levels, automating processes to streamline efficiency, and monitoring and reporting on system status.
- **Protect the infrastructure** by securing endpoints, messaging and Web environments. In addition, defending critical internal servers and implementing the ability to back up and recover data should be priorities. Organizations also need the visibility and security intelligence to respond to threats rapidly.
- **Ensure 24x7 availability.** Organizations should implement testing methods that are non-disruptive and they can reduce complexity by automating failover. Virtual environments should be treated the same as a physical environment, showing the need for organizations to adopt more cross-platform and cross-environment tools, or standardize on fewer platforms.
- **Develop an information management strategy** that includes an information retention plan and policies. Organizations need to stop using backup for archiving, implement de-duplication everywhere to free up resources, use a full-featured archive system and deploy data loss prevention technologies.

Cybercrime is an ever-evolving threat, and there is no single solution to prevent attacks. Bad actors are getting smarter and more resourceful every day and we must continue to be vigilant to protect our economy, our national security, and our way of life. Symantec applauds Congress and the Administration for focusing much needed attention on this serious issue and making it a high priority, and we look forward to continuing the important dialog around cybersecurity legislation.

Symantec would like to thank the Committee for the opportunity to testify today. We remain committed to continuing to work in coordination with Congress, the Administration, our industry partners and customers, and the public to secure the nation's infrastructure from cyber attack.

Dean Turner

Director, Global Intelligence Network Symantec Security Response

Dean Turner is the Director of the Global Intelligence Network where he manages Symantec's Deepsight Analyst teams and security intelligence and defines Symantec’s go-to-market strategy for sensor and intelligence coverage in key regional and vertical markets. Turner also manages and co-authors the Symantec Internet Security Threat Report. In this role, he coordinates the research and analysis of attack data gathered from Symantec's DeepSight Threat Management System, Managed Security Services, Business Intelligence Services and Symantec Antivirus Research Automation for use in the publication of the ISTR. Dean is also Symantec’s Canadian spokesperson for matters relating to the ISTR having done numerous print, radio and television interviews.

Turner was one of the co-founders of SecurityFocus in 1999 and served as its Director of Operations and Content until the company's acquisition by Symantec in 2002. Prior to forming SecurityFocus, Turner worked for Network Associates as their Competitive Analysis Manager for their security product line.

Turner has a broad range of expertise from Operations and Network Security to Incident Analysis. He has spoken at various Defense and Security Conferences and maintains a research interest with the academic community on such issues as Information Warfare and Infrastructure Protection.

Turner has a bachelor's degree in political science and strategic studies from the University of Calgary, Canada and a master’s degree in security studies from the University of Hull, U.K..