Security and Storage Trends to Watch

Top Internet Security Trends of 2009:

- **Malware-Bearing Spam –** Spam is usually thought of in the context of annoying, but not necessarily dangerous. However, between September and October 2009, on average, more than 2 percent of spam e-mails had attached malware; this represents a nine fold increase in the number of spam messages actually containing malware.

- **Social Networking Site Attacks Become Commonplace –** 2009 was the year attacks against both social networking sites themselves and the users of those sites became standard practice for criminals. The latter half of 2009 saw attacks utilizing social networking sites increase in both frequency and sophistication. Such sites combine two factors that make for an ideal target for online criminal activity: a massive number of users and a high-level of trust among those users.

- **Rogue Security Software** – Symantec has identified 250 distinct misleading applications that pretend to be legitimate security software—quite convincingly so in many instances—but which actually provide little or no protection and can in reality infect a computer with the very malware it purports to protect against. From July 1, 2008, to June 30, 2009, Symantec received reports of 43 million rogue security software installation attempts.

- **Ready-Made Malware –** 2009 saw malware become easier than ever to create. This was largely due to the availability of popular user-friendly toolkits, such as Zeus, that enable even novice hackers to create malware and botnets. Many ready-made threats are in reality a conglomeration of components from other more established malware. For example, Dozer, which contained components from MyDoom and Mytob. This trend has also made malware more disposable, with a threat appearing then disappearing sometimes within just a 24 hour period.

- **Bot Networks Surge** – Bot networks are quickly becoming the foundation of all cyber crime. Symantec has observed that the majority of today's malware contains a bot command and control channel. In 2009, we even saw botnet designers expand their forte by using social networking sites as communication channels.

- **Intra- and Cross-Industry Cooperation to Stamp Out Internet Threats** – With the anniversary of the first variant of the Conficker threat upon us, we're reminded of how the increasing organization and sophistication of cybercrime has led to greater cooperation among security vendors, law enforcement and Internet service providers. Examples seen in 2009 include the Conficker Working Group (CWG), the FBI's "Operation Phish Phry" bust and the Digital Crimes Consortium, which had its inaugural gathering in October.

- **Current Events Leveraged More Than Ever –** Valentine's Day, NCAA March Madness, H1N1 Flu, the crash of Air France Flight 447, Serena Williams, balloon boy and the deaths of Michael Jackson and Patrick Swayze. Each of these events along with countless others were used by malware authors and spammers in 2009 to try and lure unsuspecting Internet users into downloading malware, buying products and falling for scams. We've reached a stage where no popular story goes unnoticed, and we can expect more of the same as major world events, such as the 2010 FIFA Soccer World Cup and Winter Olympics, get nearer.

- **Drive-by-Downloads Lead the Way–** Attackers secretly infecting Internet surfers by compromising legitimate Web sites continued to grow in popularity. In 2008, Symantec observed a total of 18 million drive-by download infection attempts; however, from just August to October of 2009 alone, Symantec observed 17.4 million.

- **The Return of Spam to Pre-McColo Levels –** Symantec saw a 65 percent decrease in total spam messages between the 24 hours prior to the late 2008 McColo shutdown and the 24 hours after, resulting in spam levels dropping to just 69.8 percent of all e-mail. In 2009, however, overall spam volumes returned to an average of 87.4 percent of all e-mail, reaching a maximum of 95 percent of all messages at the end of May.

- **The Rise of Polymorphic Threats –**Polymorphism denotes the ability to mutate. Therefore, polymorphic threats are those in which every instance of the malware is slightly different than the one before it. The automated changes in code made to each instance do not alter the malware's functionality, but virtually render traditional antivirus detection technologies all but useless against them. Symantec has observed polymorphic threats, such as Waladac, Virut and Sality, become more common as online criminals seek to expand their repertoire of ways to circumvent conventional antivirus technology.

- **An Increase in Reputation Hijacking** – Geocities was a common brand name hijacked by spammers in an attempt to dupe computer users, but with Yahoo's late October shutdown of the Web hosting service, Symantec has witnessed a vast increase in the number of smaller free Web services, such as URL shortening sites, whose names, and legitimate reputations, are being abused by spammers. This has no doubt been aided by advances in CAPTCHA-breaking technology, which make it easier for malicious characters to establish multiple disposable accounts and profiles used for spamming. Symantec has even observed that some of these smaller Web services companies' sites actually shut their own sites down as the only way to stop the spam.

- **Data Breaches Continue** – As of October 13, 2009, 403 data breaches have been reported for the year, exposing more than 220 million records, according to the Identity Theft Resource Center. Well-meaning insiders continue to represent the bulk of data loss incidents with 88% of all data loss incidents caused by insiders like employees and partners, according to The Ponemon Institute. There are rising concerns, however, about malicious data loss. 59% of ex-employees admitted that they took company data when they left their jobs, according to another study by Ponemon. While organizations are increasingly focused on preventing data loss, it's clear that more needs to be done to prevent sensitive information from leaving an organization.

Security Trends to Watch in 2010:

- **Antivirus is Not Enough –** With the rise of polymorphic threats and the explosion of unique malware variants in 2009, the industry is quickly realizing that traditional approaches to antivirus, both file signatures and heuristic/behavioral capabilities, are not enough to protect against today's threats. We have reached an inflection point where new malicious programs are actually being created at a higher rate than good programs. As such, we have also reached a point where it no longer makes sense to focus solely on analyzing malware. Instead, approaches to security that look to ways to include all software files, such as reputation-based security, will become key in 2010.

- **Social Engineering as the Primary Attack Vector –** More and more, attackers are going directly after the end user and attempting to trick them into downloading malware or divulging sensitive information under the auspice that they are doing something perfectly innocent. Social engineering's popularity is at least in part spurred by the fact that what operating system and Web browser rests on a user's computer is largely irrelevant, as it is the actual user being targeted, not necessarily vulnerabilities on the machine. Social engineering is already one of the primary attack vectors being used today, and Symantec estimates that the number of attempted attacks using social engineering techniques is sure to increase in 2010.

- **Rogue Security Software Vendors Escalate Their Efforts –** In 2010, expect to see the propagators of rogue security software scams take their efforts to the next level, even by hijacking users' computers, rendering them useless and holding them for ransom. A less drastic next step, however, would be software that is not explicitly malicious, but dubious at best. For example, Symantec has already observed some rogue antivirus vendors selling rebranded copies of free third-party antivirus software as their own offerings. In these cases, users are technically getting the antivirus software that they pay for, but the reality is that this same software can actually be downloaded for free elsewhere.

- **Social Networking Third-Party Applications Will be the Target of Fraud –** With the popularity of social networking sites poised for another year of unprecedented growth, expect to see fraud being leveraged against site users to grow. In the same vein, expect owners of these sites to create more proactive measures to address these threats. As this occurs, and as these sites more readily provide third-party developer access to their APIs, attackers will likely turn to vulnerabilities in third-party applications for users' social networking accounts, just as we have seen attackers leverage browser plug-ins more as Web browsers themselves become more secure.

- **Windows 7 Will Come into the Cross-Hairs of Attackers –** Microsoft has already released the first security patches for the new operating system. As long as humans are programming computer code, flaws will be introduced, no matter how thorough pre-release testing is, and the more complex the code, the more likely that undiscovered vulnerabilities exist. Microsoft's new operating system is no exception, and as Windows 7 hits the pavement and gains traction in 2010, attackers will undoubtedly find ways to exploit its users.

- **Fast Flux Botnets Increase –** Fast flux is a technique used by some botnets, such as the Storm botnet, to hide phishing and malicious Web sites behind an ever-changing network of compromised hosts acting as proxies. Using a combination of peer-to-peer networking, distributed command and control, web-based load balancing and proxy redirection, it makes it difficult to trace the botnets' original geo-location. As industry counter measures continue to reduce the effectiveness of traditional botnets, expect to see more using this technique being used to carry out attacks.

- **URL Shortening Services Become the Phisher's Best Friend** – Because users often have no idea where a shortened URL is actually sending them, phishers are able to disguise links that the average security conscious user might think twice about clicking on. Symantec is already seeing a trend toward using this tactic to distribute misleading applications and we expect much more to come. Also, in an attempt to evade antispam filters through obfuscation, expect spammers to leverage shortened URLs shorteners to carry out their own evil deeds.

- **Mac and Mobile Malware Will Increase –** The number of attacks designed to exploit a certain operating system or platform is directly related to that platform's market share, as malware authors are out to make money and always want the biggest bang for their buck. In 2009, we saw Macs and smartphones targeted more by malware authors, for example the Sexy Space botnet aimed at the Symbian mobile device operating system and the OSX.Iservice Trojan targeting Mac users. As Mac and smartphones continue to increase in popularity in 2010, more attackers will devote time to creating malware to exploit these devices.

- **Spammers Breaking the Rules** – As the economy continues to suffer and more people seek to take advantage of the loose restrictions of the CAN SPAM Act, we'll see more organizations selling unauthorized e-mail address lists and more less-than-legitimate marketers spamming those lists.

- **As Spammers Adapt, Spam Volumes Will Continue to Fluctuate –** Since 2007, spam has increased on average by 15 percent. While this significant growth in spam e-mail may not be sustainable in the long term, it is clear that spammers are not yet willing to give up as long an economic motive is present. Spam volumes will continue to fluctuate in 2010 as spammers continue to adapt to the sophistication of security software, the intervention of responsible ISPs and government agencies across the globe.

- **Specialized Malware** – Highly specialized malware was uncovered in 2009 that was aimed at exploiting certain ATMs, indicating a degree of insider knowledge about their operation and how they could be exploited. Expect this trend to continue in 2010, including the possibility of malware targeting electronic voting systems, both those used in political elections and public telephone voting, such as that connected with reality television shows and competitions.

- **CAPTCHA Technology Will Improve** – As this happens and spammers have a more difficult time breaking CAPTCHA codes through automated processes, spammers in emerging economies will devise a means to use real people to manually generate new accounts for spamming, thereby attempting to bypass the improved technology. Symantec estimates that the individuals employed to manually create these accounts will be paid less than 10 percent of the cost to the spammers, with the account-farmers charging $30-40 per 1,000 accounts.

- **Instant Messaging Spam** – As cybercriminals exploit new ways to bypass CAPTCHA technologies, instant messenger (IM) attacks will grow in popularity. IM threats will largely be comprised of unsolicited spam messages containing malicious links, especially attacks aimed at compromising legitimate IM accounts. By the end of 2010, Symantec predicts that one in 300 IM messages will contain a URL. Also, in 2010, Symantec predicts that overall, one in 12 hyperlinks will be linked to a domain known to be used for hosting malware. Thus, one in 12 hyperlinks appearing in IM messages will contain a domain that has been considered suspicious or malicious. In mid 2009, that level was 1 in 78 hyperlinks.

- **Non-English Spam Will Increase –** As broadband connection penetration continues to grow across the globe, particularly in developing economies, spam in non-English speaking countries will increase. In some parts of Europe, Symantec estimates the levels of localized spam will exceed 50 percent of all spam.

Storage Trends to Watch in 2010:

- **2010 is the 'Year of Deletion':** Next year, enterprise IT administrators will continue to struggle with the continuing growth of information, while budgets continue to lag. The InfoPro says 2010 overall storage spending will improve over 2009, but many respondents are still expecting flat or even decreasing budgets. The last time storage technology kept up with information growth was 2002. In order to keep up, storage admins will need to begin to lose their 'pack rat' mentality and start deleting information. The 'delete' mentality will lead to a shift from using backup as the long term storage location. Backup will return to its intended use and recovery while archiving will step in to manage the long term retention and disposition of information.

- **2010 Ends the Stockpiling of Backup Tapes for Long Term Retention:** Backup is the wrong application for information retention because it is organized around information islands – systems – rather than information itself. An active, deduplicated archive with automated retention and deletion dramatically reduces the cost and time of long term information storage and retrieval. In 2010 the role of backup changes to focus on short-term recovery – fast deduplicated backups and rapid, granular recovery with built-in replication to DR sites.

- **Deduplication Everywhere**: In 2010, deduplication will become widely deployed as a feature, rather than a standalone technology. Seventy percent of enterprises still have not deployed deduplication, but will leverage easier deployments next year as it becomes built into most storage offerings – everything from backup software, to primary storage, to replication and archiving software. As more enterprises reap the benefits of deduplication and the gap it bridges with information management, the primary issue will become management of storage resources. As a result, enterprises will look to vendors to deploy simplified and cross-platform deduplication management that save time and money.

- **Industry Competition Drives Standardized Software**: Both industry consolidation and increasing industry competition will drive the need for heterogeneous standardized management software in 2010. For example, the potential Sun/Oracle merger, as well as their competition with IBM and Cisco in the integrated x86 mainframe market, will provide a variety of choices for enterprises. These options will continue to create a need for data protection, storage, and high availability technologies that eliminate information islands formed by mainframe-like vertical integration.

- **A Year of Migration:** As organizations migrate to new Microsoft platforms over the next year, they will need various storage management and data management technologies in place. While upgrading is not always a priority for IT organizations, given tight budgets and the resources needed to manage the process, newer versions can offer significant technological advancements and performance enhancements that can help organizations better meet their SLAs. As organizations migrate, they will likely make technology improvements across the board to provide improved protection and management that will support all Microsoft applications in the most efficient way. However, it is important that organizations not treat these new applications in a silo manner and apply platform level backup, deduplication, archiving, retention, and E-Discovery solutions. A trusted platform can address both new and old applications in a centralized way.

- **Virtualization Moves Beyond x86:** In 2010, more users will be able to benefit from virtualization as competition increases among providers. Not only will Hyper-V provide added functionality with Windows Server 2008 R2, IBM will likely have continued support with AIX. In 2010, it will be clear that users can leverage all flavors of virtualization, not just x86. As virtualization becomes even more widespread and prolific, users will need to implement strategies and technologies that help them to manage the entire IT infrastructure – whether physical or virtual – in a robust, yet simplified and user-friendly way.

- **Cloud Storage Catches On:** As a growing number of enterprises look for ways to improve storage efficiency and reduce management complexity of their growing environments, they look to leverage storage architecture designs already deployed by storage service and public cloud providers. Most will begin to recognize the combination of commodity hardware infrastructure and value-added software as the best approach to deliver storage to the business, but will need to decide between public, private or hybrid models. In evaluating their options, enterprise storage managers must consider the cost, scalability, availability, manageability and performance of any solution that will serve as the foundation for file-based storage services.

- **Cloud Storage Drives Data Management:** The continued move to cloud storage over the next year will drive enterprise organizations to implement more effective data management tools and strategies. While users can leverage cloud computing to ensure enhanced application performance and availability, there are also inherent risks that administrators will need to address to leverage this flexibility.

- **Organizations Can No Longer Procrastinate 'Going Green':** In 2009, organizations began to shift from implementing "green" technologies primarily for cost reduction purposes, to a more balanced awareness of also improving the organization's environmental standing. In 2010, these two drivers will push most enterprise organizations to implement a 'green' strategy. IT decision makers are increasingly justifying green IT solutions by more than cost and IT efficiency benefits. They are now looking to a number of factors such as reducing electricity consumption, cooling costs and corporate pressure to be 'green.'