As has been the case since its inception, the Internet continues to expand and enable new ways of doing business and communicating. While trends such as social networking, cloud computing, and virtualization continue to gain traction, and are rapidly becoming integral to how business and leisure pursuits are conducted online, these technological advances bring with them additional security challenges.

In today’s information-driven world, safeguarding data is a top priority. As technology evolves, it becomes more important for government organizations to know where their digital information is stored, how it is being used, and how to best prevent and protect against its loss so as to avoid downtime and loss of confidential information. This means making sure IT managers or the right government officials are aware of the latest threats and know how to protect themselves.

Unfortunately, cyber attacks and malicious activity continues to spread, and neither the economic recession nor geographic location slowed cybercriminals. Their businesses are thriving while the rest of the world suffers. Internet penetration around the world continues to increase, and as developing countries gain broadband access, cybercriminals have more markets to target.

In fact, according to Symantec’s annual Internet Security Threat Report, hacking accounted for 60 percent of the identities exposed in 2009, a marked increase from 22 percent in 2008, so it is vital all government organizations ensure they are properly protected and safeguarded from internal and external threats.

**Growth of cybercrime**

Cybercrime is a universal problem. Attackers have evolved from simple scams to highly sophisticated campaigns targeting government entities and some of the world’s largest corporations. The scale of these attacks and the fact that they originate from around the world, makes this a truly international problem requiring the cooperation of both the private sector and world governments.

In 2009, Symantec blocked an average of 100 potential attacks per second. Malicious code is as prevalent as ever, with more than 240 million distinct new malicious programs identified by Symantec in 2009 – a 100 percent increase over those found in 2008.

One of the latest threats identified by Symantec is the Hydraq Trojan (a.k.a., Aurora). This threat uses a zero-day vulnerability in Microsoft® Internet Explorer® to install itself onto a computer. Another method it uses is a social engineering ploy that relies on a maliciously coded PDF sent as an email attachment. Although a number of the command-and-control servers that the Trojan relied on for its propagation are no longer active, additional instances of Hydraq could still exist within an organization’s network. While government entities were not specifically targeted in this attack, some critical infrastructure sectors were targeted and such attacks will continue to negatively affect private sector and government organizations until they can be identified and eliminated.

**Social networking threats**

Social networking sites should be of particular concern to government organizations. Not only does social networking provide potential attack vectors for threats, such as Koobface, but if organizational policies are not established (both from an end user and network perspective), it can create security issues for the organization and its employees. This includes the potential loss of confidential information and the possible exposure of the organization to liabilities from compliance concerns. One recent example of this occurred in July 2009, when the new head of the British foreign intelligence service was identified publicly by his wife’s posts on her profile on a social
networking site.

These problems can be compounded by government organizations having differing responses to social networking. For example, the US Army has issued guidance to its soldiers as well as to civilian employees regarding social networking and what should and should not be disclosed, while the US Marine Corps has banned all access to social networking sites from its network. To effectively manage social networking within government networks, clear policies on access to these sites is required, along with appropriate countermeasures to prevent unauthorized information from being posted.

Social engineering
Another concern is social engineering, which is essentially an attempt to gain access to computers by exploiting human psychology, rather than the attacker having to hack into or physically access the computer.

While social engineering is not a new threat vector, it continues to be an area that gives attackers an avenue into enterprises and government organizations and is a primary mechanism for getting malicious code such as Trojans onto computers. An example of a social engineered attack is phishing. This is where hackers use spam, fake websites, crime-ware and other techniques to trick people into divulging sensitive information, such as bank and credit card account details. Once a hacker captured enough victims’ information, they either use the stolen goods themselves to defraud the victims (e.g., by opening up new accounts using the victim’s name or draining the victim’s bank accounts) or they sell it on the black market for a profit.

Emerging technologies
Another issue facing many government organizations is emerging technologies. While new technologies can often drive innovation, reduce costs and increase efficiency across the organization, they are equally as often not fully understood from a security perspective and could negatively affect enterprises. For example, organizations moving toward a cloud-computing model should have clear policies on what information is allowed to be uploaded by employees and to monitor it. Clear policies on usage, permissions and ownership between the organization and the ISP hosting the data should also be determined.

Virtualization is another ongoing concern for government organizations. Virtualization can be a tremendous benefit for many initiatives, including reducing the physical footprint of the enterprise and, thus, reducing both capital expenditures and energy costs. However, robust security practices need to be applied to virtual systems as much as to physical systems. This includes employing endpoint security solutions to protect each virtual host.

The underground economy
A final area that continues to be a concern is the flourishing underground economy. While there have been some successful prosecutions of underground economy operators – including the capture and guilty plea of the TJX hacker for a number of significant data breaches – highly motivated groups and individuals continue to thrive on underground economy forums.

The emergence of attack toolkits has made cybercrime available to anyone regardless of computer skills. Novices can purchase a kit and almost immediately begin deploying sophisticated and varied threats. Toolkits such as Zeus are easy to find online and can be purchased for as little as $700.

Governments need to ensure critical and sensitive information is adequately protected.

Governments need to ensure critical and sensitive information is adequately protected, and continued efforts among law enforcement needs to be coordinated to address malicious activity occurring globally. This is especially critical in the absence of an agreed-upon international framework for combating cybercrime.

Where do we go from here?
To be truly protected against today’s increasingly complex and organized cyber attacks, organizations need multiple layers of security that protects the end user from all angles and it means looking for an all-in-one suite that is easy to use and protects against malicious software, spam, data loss and downtime.

This solution should have end-to-end protection, ensuring it is sophisticated enough to defeat both known and unknown threats no matter the device (i.e., laptops, desktops, mobile devices and servers; in email; over the network; and in storage devices). The solution must also have effective and accurate anti-spam protection that automatically detects spam without requiring manual adjustment of filtering rules or monitoring of false positives. Finally, the solution should have rapid, reliable backup and archiving technology, enabling government organizations to easily archive and restore data while protecting against new threats.

Given how silent and targeted today’s attacks are, government organizations should also ensure they have a robust security information management (SIM) solution in place. This solution collects, analyzes and reports on log data and is designed to deliver proactive security protection, helping organizations demonstrate IT policy compliance and reduce overall security risk.

The effectiveness of even the best technology and processes can be undermined if employees do not understand the value of the government’s information assets and their role in mitigating risk. With heightened awareness, however, employees can also become the strongest line of defense and the most valuable security asset. This can be accomplished through formal security awareness training programs or mandating clear security policies.

With cybercriminals finding it increasingly profitable to use the Internet to steal information from consumers and businesses, protection and mitigation against such attacks becomes both an individual and collective global priority. With a proven set of technologies in place and best practices followed, the public sector can keep their information assets safe.

Marc Fossi is executive editor of Symantec’s Internet Security Threat Report. For additional information, please visit www.symantec.com