

# Information Security **An Executive Guide**

WHENEVER A MAJOR TECHNOLOGICAL BREAKTHROUGH IS ACHIEVED TO ENHANCE THE PRODUCTIVITY OF WORKERS in the digital economy, malware developers immediately begin to explore vulnerabilities and develop new threats to exploit potential weak spots. This is true for two of the most dramatic technological developments in recent years. The emergence of enhanced mobility and cloud computing are revolutionizing how organizations operate and people work. But there are steps that need to be taken to retain the benefits of these technologies while mitigating the risks. —By Bob West, CEO, Echelon One



## Companies Shift IT Resources to the Cloud, Executives Must Reassess Security Measures

**A** growing percentage of companies around the world are rapidly adopting cloud computing to support critical information technology objectives. The reasons are straightforward. Companies want to avoid unnecessary capital expenditures. In uncertain times, they want the flexibility to scale up – or down – without incurring penalties. Renting IT resources from the cloud “on demand”

**“Data, applications and intellectual property that were once carefully managed and monitored by trusted employees, now reside in a place that is controlled by a third party outside of the corporate firewall.”**

**LAURA MAIO, TREND MICRO**

of the corporate firewall,” says Laura Maio, Global Product Marketing Manager for Deep Security at Cupertino, Calif.-based Trend Micro.

Even more disconcerting is the realization that enterprise

makes both of these priorities possible. However, while moving to this new technical and economic model generates undeniable business benefits, it also dramatically alters the risk posture of important enterprise information assets.

“Data, applications and intellectual property that were once carefully managed and monitored by trusted employees, now reside in a place that is controlled by a third party outside of

executives may not have an accurate handle on the extent to which cloud computing resources are being used. Because getting access to cloud resources can be provisioned with a few clicks and a credit card, there is growing evidence that many department managers are using cloud computing providers without necessarily informing or consulting with their own IT departments.

It is important, according to Maio, to recognize that once an organization “rents” an instance of a server application, it is still incumbent upon the “renter” to assure regulators, auditors and other important stakeholders that the proper patches, updates and other security measures are properly applied. Executives, therefore must:

- Determine the actual cloud computing usage;
- Develop practices and policies that address the special security issues of resources in the cloud; and
- Deploy technologies and specific security monitoring tools that secure the cloud.

Trend Micro offers a solution called “VM Protection” that is specifically optimized for the virtualized environment of cloud computing. The technology – developed by Third Brigade, a Canadian company that was acquired this year by Trend Micro – can be used to provide immediate protection for up to 100 virtual machines and is a quick-start version of the company’s Deep Security solution.

**40 Million**  
Credit Card Numbers Stolen from TJX

**Trojan horse captures data on 2,300 Oregon taxpayers** ■ 5C

**98,930 Affected In Forever 21 Data Breach**  
*Johnson, Globe Staff*

*...your front has been active... it appears to be getting warmer by tomorrow's end.*  
continued on page 120

**Hotel Chain Falls Victim to 14,000 Data-Stealing Malware Incidents**

**University of Indianapolis Hacked: 11K Student, Faculty, Staff Records Stolen**  
4C

**6,700 Data-Stealing Malware Infections Plague US Healthcare Company**

**60% OF BUSINESSES  
ARE HIT BY CYBERCRIME.\***  
Think your data isn't as attractive as theirs?

## **THINK AGAIN.**

Data-stealing malware is on the rise. These new Web threats are stealthy, fast, and after your corporate and financial data—threatening your brand and risking your reputation. They are infiltrating the most secure businesses and yours could be next. But with on-premise or hosted solutions and services powered by the Trend Micro™ Smart Protection Network™, you'll be ready. This unique cloud-based security infrastructure protects you by blocking threats before they can reach your network and damage your business. The Trend Micro Smart Protection Network – it's security made smarter.

- ▶ Find out how secure your network really is. Register for a free onsite security assessment at [trendmicro.com/thinkagain](http://trendmicro.com/thinkagain)



Securing Your Web World

\*According to reports from the U.S. Department of Justice.  
©2009 Trend Micro Inc. All rights reserved. Trend Micro and the t-ball logo are trademarks or registered trademarks of Trend Micro Inc. All other company and/or product names may be trademarks or registered trademarks of their owners.

## Are US social sites up to the task of spreading freedom?

By Jeff Moss

Founder of DEF CON and Black Hat

Member, Homeland Security Advisory Council

WE HAVE ENTERED A NEW phase of dependence on the internet, beyond consumer oriented shopping sites, addicting puzzle places, and social networking platforms. The internet has become the default platform to rally support for political candidates, voice dissent with the status quo, expose governmental misdeeds, spread news from citizen to citizen, and plan civil disobedience.

In the United States we take for granted the protections of the 1st Amendment, and have designed our web sites accordingly, with little to no privacy protections built in. Everything has been designed to protect your credit card digits, not the expression of your communications.

This does nothing, for example, to help protect protesters in Iran who rely on U.S. social sites to spread news about their contested election. The only thing encrypted is their password when they log in to a site. After that, every post they write, every friend they make, and every gathering they plan can be recorded and accessed weeks or months later.

No major social, blog, or email site uses encryption for all their communications. On most sites it is not even an option. SSL encryption requires additional computer processor resources, but CPU power has become a cheap commodity and dedicated SSL accelerator costs are only in the hundreds of dollars. User's computers and browsers have become faster at eliminating the lag associated with the initial setup of SSL protection. It can no longer be claimed that it is too expensive an option.



# Changing Endpoint Picture Demands New Approach to Security

**E**ndpoint security used to be a fairly simple proposition; desktop terminals were protected from malicious threats by putting them behind a firewall and keeping the anti-virus profiles up to date. But then all the important things started to change.

- Companies began replacing desktops with laptops, netbooks and smartphones as the primary enterprise network access devices.
- Malware injected into cyberspace is growing at an explosive rate; hackers are introducing up to 2000 new malware threats per hour.

“Security threats to the endpoint have evolved significantly in recent years, and many organizations probably need to update their strategies for securing critical endpoint assets,” says Christine Drake, Global Senior Product Marketing Manager for Enterprise Endpoint Security at Cupertino, Calif.-based Trend Micro.

The traditional way of mitigating threats to the endpoint revolved around identifying a signature for each attack, and then sending a profile to every endpoint in the enterprise. This prevented code containing malware signatures from being executed in the system. But if security departments continue this practice the following can occur:

- Once-a-day updates become obsolete within minutes of being installed;
- The file size of daily signature updates become larger, taking longer to update while diminishing computer or device performance; and/or

- Staying current requires more frequent updating, affecting bandwidth throughput on the enterprise network.

Given the current volumes and the fact that it is projected to continue exploding, the current security model for endpoint security is just not sustainable.

“That is why Trend Micro believes that it is important to shift more of the security work to the ‘cloud,’” explains Drake. “With a cloud-

**“Security threats to the endpoint have evolved significantly in recent years, and many organizations probably need to update their strategies for securing critical endpoint assets.”**

**CHRISTINE DRAKE  
TREND MICRO**

client architecture, the clients simply query cloud-based global threat intelligence that correlates email, web, and file reputations – blocking malware and dangerous web pages before they even touch users’ terminals. And users can access this protection when both on and off the network, securing mobile and remote workers. With in-the-cloud correlated threat intelligence it is possible for the entire community of users to benefit immediately from the identification of rogue code and web sites – or compromised pages within legitimate web sites – while minimizing the impact on network and endpoint performance,” she says.



For more information visit: [www.trendmicro.com](http://www.trendmicro.com)