

March 2008

February 2008

January 2008

December 2007

November 2007

October 2007

September 2007

August 2007

July 2007

June 2007

May 2007

April 2007

March 2007

February 2007

Prior SecureNews issues

SecureNews subscription form

March 2008 *Secure Computing® brings you the latest SecureNews.*

See left column for March Table of Contents.



[Come See Secure Computing at the 2008 RSA Conference!](#)



Table of Contents

In this SecureNews:

Breaking news

[Come See Secure Computing at the 2008 RSA Conference!](#)

~ [Secure Computing Partner Program Wins VARBusiness Gold 5-Star Award](#)

~ [Visit Secure Computing at Infosecurity Europe - April 22-24 2008](#)

~ [Secure Computing Web 2.0 Security Lunch & Learn Series Expands to 10 More Cities](#)

SecureAlerts

~ [Federal Agencies in Peril](#)

~ [Over 10,000 Web Sites Infected](#)

Secure Computing® is a Sponsor at **The RSA® Conference** April 8 – April 10, 2008 at the Moscone Convention Center in San Francisco.

VISIT US IN **BOOTH # 1017** on the main show floor near the entrance, and participate in the Secure ULTIMATE CHALLENGE GAME!

FOR COMPLIMENTARY RSA Conference Expo passes visit [this site](#) before April 4, 2008, and pre-register using the registration qualification code - EXH8SCC. You can pick up your badge on site!

SHOW DATES AND HOURS:

Tuesday, April 8	11:00 AM – 6:00 PM
Wednesday, April 9	11:00 AM – 6:00 PM
Thursday, April 10	10:00 AM – 4:00 PM

COME HEAR OUR EXPERTS!

The Role of Internet Reputation Intelligence in Critical Infrastructure Protection

Speaker: Phyllis A. Schneck, Ph.D.
Scheduled Date: Tuesday, April 8, 2008
Scheduled Time: 1:30PM
Location: Executive Briefing Center

Organized Online Criminal Enterprises: Profile of Who, Where and How

Speaker: Dmitri Alperovitch
Scheduled Date: Friday, April 11, 2008
Scheduled Time: 9:00AM
Location: Green Room 104

Secure Solutions

- [On Demand Webcast: PCI DSS – Your Stepping Stone to a Trusted Security Model](#)
- [Catching Spies with Secure Web \(*Webwasher*\)](#)

Product corner

- [Secure Computing Announces New Product Brands](#)
- [Secure Computing Announces the Release of Secure Mail 6.5.4](#)
- [On Demand Webcast: Techniques to Stop Unfiltered Internet Access through Anonymous Proxies](#)
- [University of Minnesota Protects Privacy, Keeps Data Secure with Secure SafeWord](#)
- [Crowne Plaza Hotels and Resorts Implements Secure Web](#)

Worldwide news

- [SecureNews Monthly Press Highlights](#)



Secure Computing Partner Program Wins VARBusiness Gold 5-Star Award



Secure Computing is pleased to announce that it has been recognized by CMP Channel's VARBusiness as one of North America's top information-technology (IT) vendors for its PartnersFirst program.

Secure Computing was certified as a Gold 5-Star Overall Winner in the VARBusiness 2008 Partner Programs Guide (PPG), a guide that acknowledges the commitment and strength of a vendor's partner programs for its Channel resellers, IT integrators, and technology consultants.

The goal of the Secure Computing's PartnersFirst Program is to enable partners to successfully deliver superior security solutions to their customers. The company connects partners to a wealth of resources aimed at increasing customer satisfaction and partner profitability. And the program provides partners with the key ingredients for success; starting with excellent profit margins, this includes joint marketing opportunities, best-in-class training and technical support, sales tools, and much more.

Of the hundreds of vendor program entries reviewed for this year's guide, Secure Computing was one of only ten Gold 5-Star Overall Winners chosen in this 14th annual VARBusiness Partner Programs Guide survey. Secure Computing was also certified a Silver 5-Star Winner in the categories of Sales Support, Marketing Support, Channel Operations, and Partner Recruitment. Learn more about Secure's award-winning PartnersFirst program.



Visit Secure Computing at Infosecurity Europe - April 22-24 2008

Grand Hall, Olympia, London, UK. Stand F125



Infosecurity Europe is Europe's most comprehensive convergence of information security professionals. It addresses today's strategic and technical issues in an unrivaled education program and showcases the most diverse range of new and innovative products and services from 300 of the top suppliers on the show floor. *If you are responsible for implementing, planning or managing information security – visit Secure Computing at Infosecurity Europe!* **Register before April 18th to obtain your free visitor's pass.**

[Register for your FREE Infosecurity Europe pass here](#)



Secure Computing Web 2.0 Security Lunch & Learn Series Expands to 10 More Cities

Lunch & Learn with Secure Computing



You're invited to join Secure Computing for lunch while we share with you cutting-edge information about the latest Web 2.0 security threats. Discover how companies are successfully addressing these threats through the Secure Web 2.0 Anti-Threat Initiative - SWAT.

Due to popular demand, we've expanded this series to 10 more cities in April and May. **Sign up** to attend this informative event in a city near you.

DATE	CITY
4/02/2008	Arlington, VA
4/15/2008	Portland, OR
4/16/2008	Portland, ME
4/17/2008	San Antonio, TX
4/23/2008	Austin, TX
4/24/2008	Philadelphia, PA
5/13/2008	Toronto, ON
5/14/2008	San Diego, CA
5/21/2008	Providence, RI
5/22/2008	Calgary, AB

Looking for more information about Web 2.0 threats and protection strategies? Check out our **Secure Web 2.0 Anti-Threat site**.

A Senate subcommittee hearing held on March 12 discussed the progress and shortcomings of the Federal Information Security Management Act (FISMA). According to Sen. Tom Carper (D-Del), chairman of the Subcommittee on Federal Financial Management, Government Information and International Security, sensitive information has been compromised, stolen, or improperly protected. Sen. Carper called for the March hearing, titled “Agencies in Peril: Are We Doing Enough to Protect Federal IT and Secure Sensitive Information”, to examine how well government agencies have fared in reducing security risks as required by FISMA.

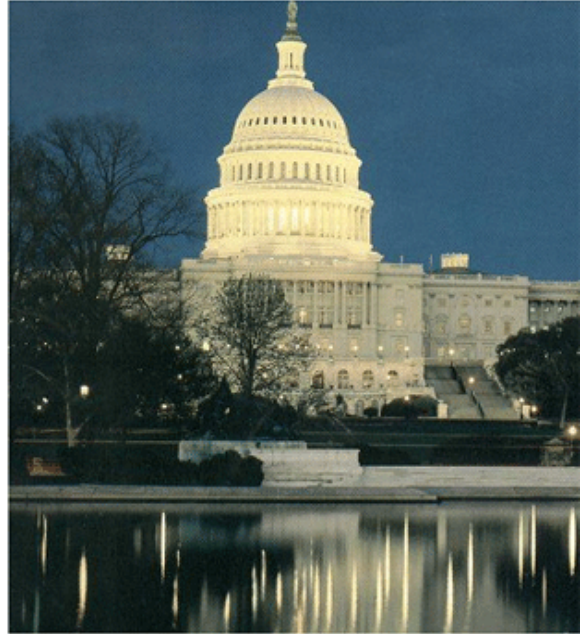
FISMA was created to strengthen security in federal civilian agencies, by requiring agencies to implement security policies and technology to reduce vulnerabilities. Agencies are required to submit for regular assessments and reviews.

According to Sen. Carper, “agencies still cannot say whether their information systems containing millions of American’s personal data are secure,” and concludes that “our information networks are not as secure as we may think.”

Some of the criticisms of agency compliance initiatives indicate that compliance does not necessarily mean increased security; instead, there is a greater focus on producing paperwork. Tim Bennett, CSIA President, testified at the hearing, saying that although some improvements have been made, **there are still significant vulnerabilities that need to be addressed and the time for strengthening FISMA is at hand.** Bennett spoke of the shocking pace of infiltration of government networks, **citing press reports of attackers working through Chinese Internet servers against federal agencies, where hackers penetrated federal systems using rootkits to steal information.** Bennett noted in his testimony that Department of Homeland Security logged 844 cybersecurity incidents in 2005 and 2006.

Although FISMA has been successful in getting federal agencies to pay more attention to security, **agencies still averaged a “C-“ on their 2007 information security report cards, based on FISMA audits.**

[Find out more about Secure Computing’s FISMA solutions](#)



SecureAlerts

Over 10,000 Web Sites Infected

According to a report on the **SANS Internet Storm Center** this month, **over 10,000 web pages** were infected with a JavaScript code that **steals passwords to online games**. The attack is similar to one used **before the 2007 Super Bowl**, which targeted visitors to the **Miami Dolphins team and stadium Web sites**.



The attack tends to target already known vulnerabilities. According to the SANS report, **the attack places active code on legitimate Web sites**, which then redirects visitors to a malicious China-based site at 2117966.net, which then **installs a password-stealing program onto the victim's computer that attempts to steal passwords for several different online games**.

The **attack is fairly unsophisticated and targets known vulnerabilities in Windows and other applications**, for which patches have already been released. Users with up-to-date patches will not be vulnerable.

Attackers often target online game passwords, since they can be sold for cash. The attack illustrates the need for a unified approach to security. Because the attack focuses on infiltrating known and trusted Web sites, traditional Web filtering solutions may still allow the attack to take place.

Interested in more information on security issues and solutions? Check out Secure Computing's comprehensive collection of **white papers**.

SecureSolutions

On Demand Webcast: PCI DSS – Your Stepping Stone to a Trusted Security Model

In this presentation to ISSA members, Secure Computing's Elan Winkler provides a **status of the current adoption of the PCI standard**. In addition, Ms. Winkler also discusses **how to use PCI as a stepping stone to create a culture of compliance** - one that's built on a trusted security model. This trusted security model enables enterprises to protect their data, their people and their infrastructure with easy-to-deploy and manage technology.



View this free webcast now

To learn more about Secure Computing's PCI solutions, visit our **PCI site**.

#1 Rated Anti-Malware/Anti-Spyware Protection

Do you think that nobody would be interested in spying on your network? Think again.

Spyware has become a major threat to enterprise network security, and according to IDC, 67 percent of all computers have some form of spyware.



If you run the nation's Defense network, protect the Colonel's secret recipe, or are the guardian of the Internet's "Next Big Thing," it's likely that you're worried about spies, and you would be right to be paranoid. **But spyware isn't just about stealing the big secrets of the world, it's all about the little things. Spyware pilfers your passwords. It's a kleptomaniac of keystrokes; it's a shady salesman with a loud tie lurking inside your computer waiting to see where you've surfed.**

And just like a good spy with a briefcase full of fake moustaches, spyware takes many forms. **Download this paper to read how Secure Web products stop spyware and malware cold, backed by its #1 anti-malware rating, blocking 99.83% of malware in recent independent studies.**

[Download paper now](#)

Product corner**Secure Computing Announces New Product Brands**

Secure Computing recently announced the launch of the Company's new set of product brands meant to improve overall awareness of Secure Computing Corporation and the integrated solutions it offers. The new branding system, which includes a new corporate logo and [company website](#), simplifies and unifies the look and feel across all product and platforms to better communicate important characteristics and values to the market.

All Secure products now fall under a common nomenclature that emphasizes the integration done across all products and that they are part of the "Secure" product family. The main product lines have been renamed as follows:

- IronMail® is now "Secure Mail"
- Webwasher® is now "Secure Web"
- Sidewinder® is now "Secure Firewall"
- SafeWord® is now "Secure SafeWord"
- SnapGear® is now "Secure SnapGear"

To efficiently execute this, the company will implement an immediate roll-out of the new product names while also connecting them with the previous names on the corporate Website and in product documentation. For

example, when discussing the “Secure Firewall”, the company will leave a single reference to the “Sidewinder” solution. Thereby simultaneously leveraging old-brand familiarity and attaining new brand acceptance, while drawing a bridge between the two, and at the same time avoiding any disruption of business.

For more information on Secure Computing products, please see our updated [Products at-a-Glance Overview](#).



Secure Computing Announces the Release of Secure Mail 6.5.4

Secure Computing is pleased to announce the release of Secure Mail (*IronMail*) 6.5.4, our award-winning mail security appliance. Secure Mail 6.5.4 is an upgrade from Secure Mail 6.5.3, and includes all new features, enhancements, and hotfixes from previous versions of Secure Mail.



The following are some of the key features and upgrades included in Secure Mail 6.5.4:

PROTECTION/SECURITY FEATURES

- **LDAP Connection Control (directory harvest protection):** Protects customer directory structures from spammers attempting to harvest their user information and also increases spam blocking effectiveness.
- **DSN bounce verification protection (backscatter protection):** Bounce Address Tag Validation (BATV) filters invalid bounce messages sent to forged addresses, preventing “joe job” spam and DoS attacks.
- **Image Spam Classifier updates:** New ISC libraries improve image spam detection and reduce false positives.
- **Dynamic Spam Classifier:** DSC provides fast-reaction detection methods to Secure Mail to fight new spam outbreaks.

MANAGEMENT FEATURES

- **Automated whitelist expiration:** Administrators can configure automatic expiration and deletion of whitelist rules that are no longer in use to maximize appliance performance.
- **SNMP polling:** Provides the capability for a polling station or package to collect data from the Secure Mail appliance and map alert events via the SNMP protocol.
- **End User Quarantine unique links:** Users have a unique link for accessing their quarantined messages, rather than receiving a new link each time they get EUQ notices. The Administrator can control the expiration frequency and refresh the link at any time.
- **Message Blocking Report:** This report provides a simple Total Messages Summary for quick review, followed by a detailed report that shows messages blocked by each Secure Mail feature.
- **Validation algorithms additions:** Mod 10, CUSIP, and ISIN regular expression validation ensure sensitive data doesn’t leave through customer email systems, such as credit card numbers and critical banking routing information.

For complete information regarding Secure Mail version 6.5.4, including additional details on these and other new features, see the [full release notes](#).

[Find out more about our Secure Mail solutions](#)



On Demand Webcast: [Techniques to Stop Unfiltered Internet Access through Anonymous Proxies](#)

Are your users finding ways around Web filtering? There are a number of options and tools for circumventing Web filtering today such as Web sites that allow anonymous surfing and Web-based anonymous proxies that allow unfettered access to the Web through a home or off-site computer. **Learn more about how individuals are circumventing Web filtering solutions and how you can solve the problem.**

Join Secure Computing filtering expert, Tom Bryant, for an informative Webinar to learn techniques you can implement to keep your Internet traffic filtered.

[View this webcast now](#)



[University of Minnesota Protects Privacy, Keeps Data Secure with Secure SafeWord](#)



When the University of Minnesota saw the need to strengthen their authentication system, they realized that passwords—no matter how strong—are still vulnerable. After a detailed study of vendors, the University deployed Secure Computing's Secure SafeWord, taking advantage of Secure's private label program to brand the Secure SafeWord Silver tokens with custom University colors. The new two-factor authentication system integrates with Web applications already in place, is much easier to manage across a large university environment, and avoids the user frustration and administrative overhead of frequent password changes.

[Read the Univ. of Minn. case study here](#)

Product corner

Secure Web

Crowne Plaza Hotels and Resorts Implements Secure Web



Crowne Plaza Hotels and Resorts has implemented Secure Computing's Secure Web (formerly known as Webwasher) to defend against Web 2.0 threats and ensure regulatory compliance.

Secure Computing's Secure Web has been implemented in Crowne Plaza hotels in Ireland to protect the organization from Internet threats through the scanning of all inbound and outbound traffic for viruses, malware and other offensive content. It is also being used to filter employee Web access to ensure safe and appropriate usage, and help to ensure the organization complies with industry regulations.

"Secure Computing's Secure Web was quick to implement and easy to manage, and is extremely effective at protecting us from targeted malware attacks."

[Read the press release](#)

Worldwide news

SecureNews monthly press highlights

Is your organization required to comply with PCI requirements? In this article in the **Sarbanes-Oxley Compliance Journal**, Secure Computing technology evangelist Paul Henry explains how the PCI DSS requirement for application level firewall falls short and **why packet filter firewalls with Layer 7 signatures are inadequate for the protection of credit card data**. Also, this month Paul details why using Skype in the Enterprise is like opening Pandora's Box from a security perspective. In this **Computer Technology Review** article, he outlines the **inherent risks of Skype and why it should not be used anywhere inside of a corporate environment**. Finally, in this **USA Today** piece, Secure Computing's principal researcher Dmitri Alperovitch talks about why **botnet scams are exploding** and why the Storm worm remains the largest, most active botnet clogging the Internet more than a year after it first appeared.

