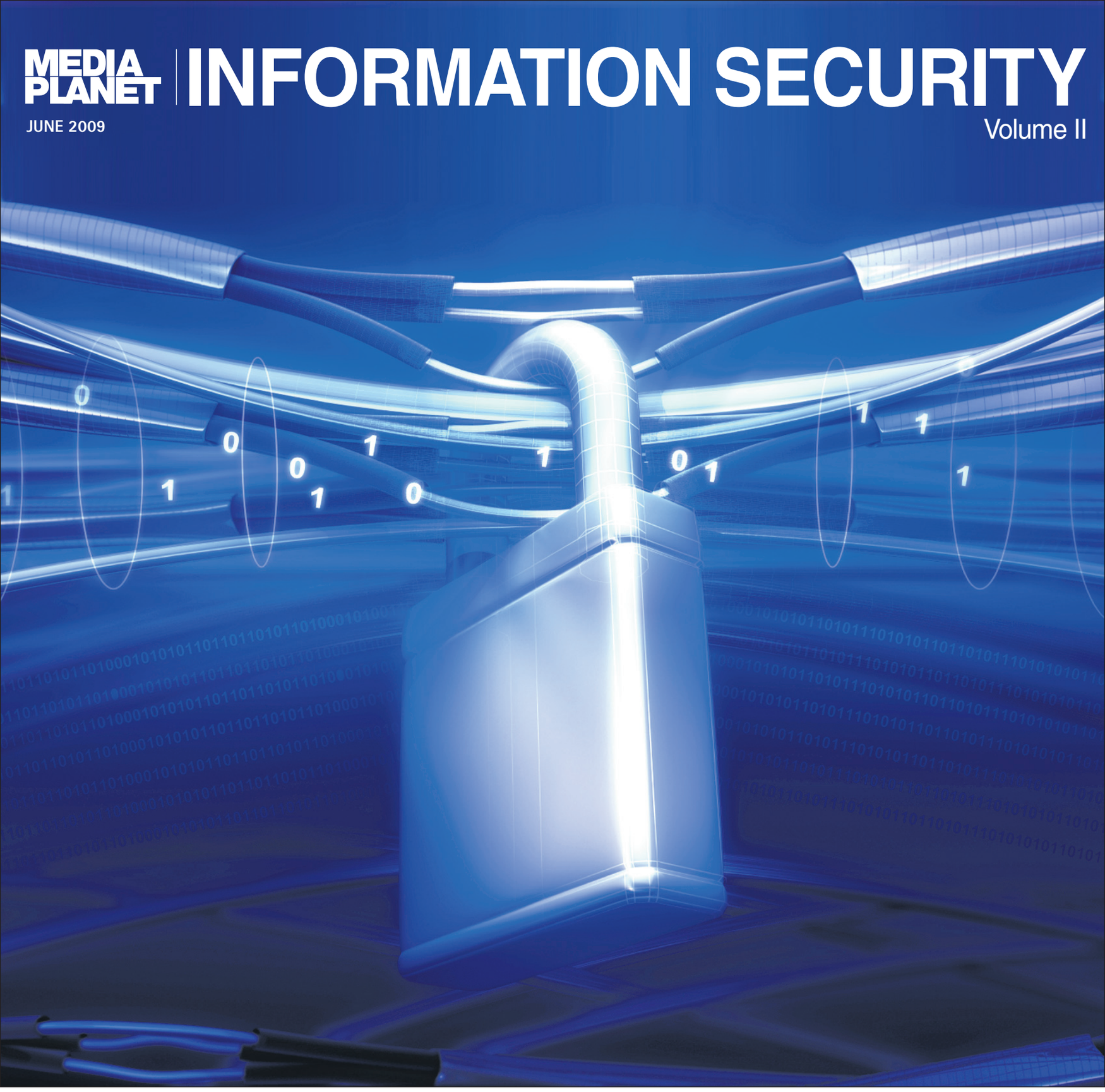
MEDIA PLANET

INFORMATION SECURITY

JUNE 2009

Volume II



MEDIA PLANET

CONTENTS

Publisher: Max Friend
max.friend@mediaplanet.com

Editorial Contributor: David Duffy
Design: Jez MacBean
Printer: Washington Post
Photos: ©iStockphoto.com

MediaPlanet is the leading publisher in providing high quality and in-depth analysis on topical industry and market issues, in print, online and broadcast.

For more information about supplements in the daily press, please contact Kayvan Salmanpour on
+1 646 922 1400
kayvan.salmanpour@mediaplanet.com

This section was written by MediaPlanet and did not involve The Washington Post News or Editorial Departments.

www.mediaplanet.com

Combating Cybercrime in an Information-Driven World

Not only has information technology revolutionized the way we live, work, and play, it has also changed the way crimes may be committed. The same digital infrastructure that we rely upon has also given rise to a thriving underground economy that is mature, professional, efficient, and profitable.

In this clandestine marketplace, cybercriminals from around the globe buy, sell, and trade millions of dollars worth of stolen goods as well as services and tools designed to facilitate online theft and fraud. For example, some cybercriminals might choose to advertise or buy stolen identities, credit card information, or bank account data. They even offer discounts for bulk purchases. Others might provide services, such as cashing out financial accounts to untraceable locations online in just minutes. Still others might sell malicious tools, including botnets, vulnerability scanners, and vulnerability exploit kits. This commerce creates income-generating opportunities throughout the supply-and-demand chain of the underground economy and ultimately increases the risk to the global economy.

Regardless of their role in the underground economy, cybercriminals are after the same thing: end-user data, from full identities complete with name, address, and Social Security number, to email addresses and passwords, banking credentials, and credit card numbers with CVV2 details. In 2008 an astonishing 78 percent of threats to confidential information exported user data, according to the latest volume of the *Symantec Internet Security Threat Report* (ISTR), which provides an annual overview and analysis of worldwide Internet threat activity and a review of the Internet threat environment. This data could be used by cybercriminals to steal an identity or to help them launch additional attacks.

Enrique Salem, President and CEO, Symantec

The success of the cyber underworld hinges on the collaboration and cooperation of individual cybercriminals as well as crime syndicates operating from virtually anywhere an Internet connection can be found. And, as more and more countries extend their broadband infrastructures, cybercriminals will gain an even larger pool of potential victims and business partners.

The most effective defense against cybercrime will require the combined efforts of individual users as well as businesses, government agencies, and schools and universities. Thanks in part to many public/private partnerships such as the National Cyber Security Alliance (NCSA) and Internet Keep Safe Coalition, tips for safely navigating cyberspace are available from the convenience of virtually any browser.

Technology providers, too, are working aggressively to deliver better protection. Through increasingly sophisticated yet easy-to-use products and services that safeguard consumers and businesses against evolving internal and external cyber threats, regardless of the computing device they are using and the network they are on, Internet users have a powerful ally in the fight against cybercrime. And new platforms and methods for securely storing and using data are continually emerging, while next-generation information management frameworks now make it easier for organizations to enforce compliance with the many industry and government standards designed to protect them.

The naming of a cyber security czar by U.S. President Barack Obama will go a long way in facilitating the coordination of a public/private partnership by fostering greater information sharing between private business and government agencies in the U.S. The designation of a cyber security coordinator, together with the proposed near-term action plan aimed at supporting U.S. cyber security policy, will help focus efforts by the federal government to invest more resources into cyber security research and development projects shared by a public/private partnership. Moreover, the appointment of a cyber security policy official will lend the weight of the White House towards more cooperation among business and law enforcement to address cybercrime on an international scale.

As individuals and organizations in the public and private sectors work together to fight cybercrime and are supported by government leaders around the world, the global online community can confidently maximize the opportunities and benefits the Internet provides.

PC MAGAZINE EDITORS' CHOICE

Sept. 9, 2008
Norton Internet Security 2009

PCWorld

February 2009
Top Internet Security Suite
Score: 89 (of 100)
Norton™ Internet Security 2009

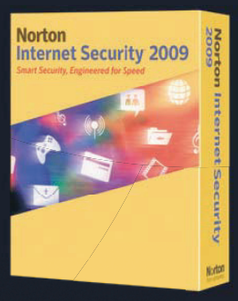
"NORTON INTERNET SECURITY 2009 WAS THE CLEAR WINNER IN THIS YEAR'S ROUNDUP OF NINE SECURITY SUITES... IT'S OUR TOP PICK."

- Erik Larkin, PC World

IF YOU WANT THE SECURITY THAT HAS EVERYONE TALKING, YOU NEED THE SPEED OF NORTON 2009.

When it comes to the fastest online protection available, experts can't stop going on about the award-winning speed and power of Norton™ Internet Security 2009. Brought to you by Symantec, the company that protects 99% of the Fortune 500®, Norton 2009 is the one security solution that keeps the industry talking and our competition speechless.

See how Norton outperforms the competition at norton.com/speed



Norton™
from symantec

SMART SECURITY, ENGINEERED FOR SPEED

Cyber Wars Fought on New Battlefields

From the gateway to the cloud, it's all about knowing your enemy

If there was any doubt left, the news that the White House is naming a "cyber czar" and the Pentagon is creating a new military cyber command should have dispelled it. We are living in the age of cyber warfare.

Consider the following: cyber attacks forced the FBI and the U.S. Marshals to shut down part of their computer networks last month. In May, the *Wall Street Journal* reported the Defense Department detected 360 million attempts to break into its network in 2008 (compared with six million in 2006). Cyber crooks have penetrated both the U.S. electricity grid and the Pentagon's biggest weapon program. The Department of Transportation's inspector general says the U.S. air traffic control system is vulnerable to cyber attacks. Then, of course, there was Georgia.

"That was the wake-up call, if we needed one," says Darrell Covell, founder and chief technology officer of Rsignia, Inc., a network security and protection company active in cyber defense. "Russian cyber gangs shut down that country's entire infrastructure. It's the current case study for cyber warfare capabilities."

The United States has significant cyber warfare capabilities – both defensive and offensive – and companies like Rsignia are working with government departments and agencies to improve current cyber defenses and develop new resources. One critical area, of course, is controlling access. The Office of Management and Budget's Trusted Internet Connections (TIC) program is reducing the federal government's connections, or access points, to the Internet from the more than 4,300 in January 2008 to fewer than 100. "You just can't secure that many gateways," says Gary Woods, Rsignia's director of federal sales for engineered solutions. But with a manageable number of access points, applications like ones developed by Rsignia can screen prospective entrants, including those using "spoofed" Internet protocol (IP) addresses to disguise their true identities. "When the UPS man shows up at your door, maybe he's for real, and maybe he's someone else entirely," Woods says. "We can strip off the uniform and look deeper into the protocols to decide whether to let the guy in, block him – or let him in and gather intelligence about who he is and what he wants."

It's also possible to see what he takes with him when he leaves and track where he goes. That kind of intelligence is a big part of being prepared and ultimately winning a cyber war. As Covell puts it, "Once you find a snake in the grass, why wouldn't you want to see what he's up to?"

Cyber attacks come in many forms, and attackers have a wide range of motives – political, financial, philosophical, organizational, etc., and some are just plain ticked off. Today, just about any business is a potential target. According to Paul Sop, Chief Technology Officer at Prolexic Technologies, a firm specializing in network protection services, the most debilitating form of cyber attack is the distributed denial of service (DDoS) attack, in which thousands of hijacked PCs are assembled into a "botnet" and can be used to bombard the target with Internet traffic to the point where legitimate visitors can't get through. DDoS attacks were used against Georgia last year, and they effectively took the Baltic nation of Estonia off line during a dispute with Russia in 2007. These attacks are increasingly large and intelligent by design, global in nature, and generally difficult to trace back to the source of the attacker(s).

The problem, in a nutshell, says Sop, is that it's "many against one. These days, any motivated attacker can download botnet building programs from the Internet. A person with the right skills can easily assemble a botnet of 10,000 or 20,000 computers in a day, and these botnets can't be disabled fast enough. Ultimately the best strategy is to develop a capability to defend against these DDoS attacks." Prolexic's solution engages the enemy "in the cloud," close to the attacker, and takes advantage of Internet routing protocols to divert all the traffic headed for a particular site to globally-distributed scrubbing centers that act as "black holes," where malicious attack traffic is inspected, filtered, separated from good traffic and blocked - all in real-time.

"Prolexic technology makes it seem like your web site is global and massive -- impossible to take down," Sop says. "Then we have experts who use some pretty incredible technology to prove the requests are from real people, not botnets. We're fighting the attackers and the attacks they launch. This game is as much about psychology as it is technology. Attackers are always at work inventing new strategies. It's our job to stay ahead of them."

iKeepSafe℠

New Education in Virtual World for Kids

Children today grow up in a world where online activities can materially compromise the security of home and school computers. For many users, computer security is an unwelcome necessity, and when security measures are finally in place, the last thing the semi-savvy user needs is a child pushing the limits of connectedness.

Many parents and educators are unprepared to help children navigate online security hazards. More than 60% of educators do not know how to teach students about detecting and minimizing viruses (NCSA 2008). "Children need early security training," says iKeepSafe president, Marsali Hancock. "Illegal downloading of music and games begins in fourth grade; cyber-bullying in second [RIT 2008]. Nothing will un-do a parent's best security efforts like a kid trying to illegally download a game or song. "

With these trends, parents and educators are turning to the next generation in social networking where kids learn essentials of cyber-security and ethics in their favorite setting—a virtual world. WoogiWorld, identified by Parents Magazine as one of the top five next generation sites for kids, has educators and kids alike flocking to this new approach to education.

WoogiWorld CEO Scott Dow tells parents and educators, "WoogiWorld is much more than fun and games; students learn core academic subjects, health, nutrition, music and art. Our unique approach succeeds through a crossover of online and offline activities. 'Woogies' earn 'Watts' [the currency of this virtual world] by completing important tasks in the real world." Children learn to balance screen-time with real life, to be active in their communities and helpful at home.

For more information, go to: www.ikeepsafe.org/woogiworld

Controlling Access While Controlling Cost

New app is easy for users too – a key criterion

Human nature being what it is, network security often has as much to do with ease-of-use as it does with passwords and protocols. With the economy in its current state, not adding cost helps too. "We bring higher levels of security to the organization and convenience to the end user," says Dan DeBlasio, director of business development, Identity and Access Management (IAM) for the Americas, at HID Global, the trusted worldwide leader in providing solutions for the delivery of secure identity.

The launch in March of HID on the Desktop™, which includes the new naviGO™ software, an HID technology card and an OMNIKEY® reader, is an example. The challenge was providing companies "two-factor" user authentication capability (access card and PIN) for desktop and laptop computers, without issuing new "smart cards" to every employee.

The answer lay in enabling existing HID access control credentials – some 300 million have been issued worldwide – to log onto Microsoft Windows. The naviGO application allows badge-holders to manage their enrollment and establish PINs, and provides for access through knowledge-based authentication when cards are lost or forgotten.

"A risk-appropriate solution," DeBlasio says. "The infrastructure was there, and we weren't adding a large amount of burden."

Dynamic Risks Demand Vigilance that Goes Beyond Compliance

As threats to information grow, more comprehensive solutions are warranted

If your company has a computer network, you don't just have a security risk. You have a dynamic security risk, that is, one that changes and evolves every hour of every day as the network itself changes with new users, new visitors, new applications and new information, and the makeup of the Internet itself evolves, at a massive rate of speed and complexity.

According to the most recent Internet Security Threat Report by Symantec, the number of new malicious code signatures on the Internet increased 265 percent in 2008 to more than 1.65 million. As the attacks and attackers both become more complex and sophisticated, their most common goal remains constant – financial gain. The Symantec report found that 78 percent of confidential information threats in 2008 exported user data. A February 2009 Symantec white paper on "Web Based Attacks" found that just about any Web site today can be compromised by cyber crooks.

"Too often we tend to think in terms of 'information security,' which is a compliance driven posture, as in, I've done everything required to make my information secure," says Jim Butterworth, senior director of cybersecurity for Guidance Software, a provider of cybersecurity, eDiscovery and other digital investigation solutions. "We should think in terms of 'cybersecurity,' which means monitoring the operations conducted on your network 24/7/365."

It's a fact of Internet life that the bad guys keep getting more insidious, as do the malicious attacks they launch. According to Butterworth, operating systems won't always recognize that someone has inserted a new piece of malicious software. One current hacker favorite is the malware that enables the so-called "drive-by download." It sits on a Web site the attackers have compromised and looks for vulnerabilities on visiting computers. When it finds one, it deposits more malware designed to steal the visitor's personal information. The visitor doesn't have to do a thing to launch the attack, and without vigilant monitoring, the owner of the web site will not be aware anything is amiss.

GUIDANCE SOFTWARE

This is where companies like Guidance Software can help. "We have over a decade of experience in digital forensics," says Butterworth. "We're used to complex problems. We've lived in a binary world so we know what it looks like – or should look like. We've designed our applications to recognize things an operating system maybe won't."

About thirty percent of Guidance Software clients are government departments and agencies, such as the Departments of Defense, State and Justice, and the SEC. One factor companies looking to enhance network security should bear in mind – the need to protect evidence in a forensically sound manner. In addition to its EnCase Cybersecurity software solution, the company's professional services organization assists with digital investigations. As Butterworth puts it, "At the outset, we don't know whether we ultimately will be looking to assist in the termination of an employee, litigation against a competitor, or the incarceration of a criminal. We do know we're likely to end up in court, and that means the investigation can't contaminate the evidence. We don't change anything. We maintain a sound environment."

Jim Butterworth, Senior Director of Cyber Security, Guidance Software, Inc.

2009 Gartner Security Summit Focuses on Network and Career Security

Information security needs are growing faster than ever as challenges and solutions become more complex.

At the same time, the economy is applying the heaviest budgetary pressure in decades. The 2009 Gartner Information Security Summit, June 28-July 1 in Washington D.C., focuses on the IT security professional and how they can optimize their value while enhancing their skills and knowledge to better protect their organization in tough economic times.

ANALYSTS

"Our team of analysts, led by conference chairs, Vic Wheatman, Chris Byrnes and John Pescatore, will concentrate on the tools, technologies and management practices that are needed to run a security operation that's efficient, safe and economical," said Alwyn Dawkins, senior vice president, events, at Gartner, Inc. "The program includes privacy policies and privacy protection tools and emerging trends and new federal initiatives regarding cyberspace."

Dawkins recently offered some advance insights on what else to expect at the 2009 Summit.

Q. Who should attend?

A. Anyone with an interest in enterprise-wide security and critical infrastructure protection. CIOs, CSOs, CISOs and CTOs, of course. But also other IT executives, network managers, risk managers, and auditors. Because of the pervasiveness of the Internet in business today, just about any senior executive will find value. Since we're in Washington, we included a special segment for people working in the public sector and a suggested agenda for government attendees.

Alwyn Dawkins, Senior Vice President, Gartner Events

Q. Tell us a little about the overall agenda.

A. There are more than 100 sessions on an incredible range of topics, all geared toward protecting your IT infrastructure, keeping your business secure, and managing your career in a time when it will clearly be affected by both technology trends and economic dynamics. We're excited by our outside keynote speaker, David Sanger of the *New York Times*, who's just published a thought-provoking book that's already climbing the best-seller charts on the challenges facing the new administration in cyber space. We'll also have a keynote panel on national cyber security strategy at a time when the president and the secretary of defense have put this issue front and center on the national agenda.

Q. What about some of the smaller sessions?

A. We're seeing a lot of interest in cloud computing and government security issues, managing costs and maximizing value, and a case study on the costs and cures of data breaches with the CEO of Heartland Payment Systems. There are also 16 analyst/user roundtables, with 12 to 15 participants, allowing for give and take with those who share an interest in a particular topic.

Attendees are eligible for CPE credits (ISC2/CISSP and ISACA). Incentive pricing available. More information at www.gartner.com/us/itsecurity

Practicing Preventative Medicine for your Network

Consider a CAT scan for your computer network. Just as preventative medicine is critical to health care, examining your computer, network, or data system for vulnerabilities is essential to keeping it safe from digital viruses and a host of other threats.

Billy Austin, chief security officer of Saint Corporation, which provides vulnerability assessment and penetration testing tools, says 15 new network vulnerabilities are disclosed every day – that's almost 5,500 a year – and those are only the ones that are made public. Some lead to large scale damage. By the end of 2008, the Downadup (also known as Conficker) worm had exploited a single vulnerability to infect more than a million individual computers, according to Symantec's most recent *Internet Security Threat Report.*

VULNERABILITIES

Software provided by Saint Corporation can run the equivalent of a CAT scan on a single computer or multi-machine network and show all the vulnerabilities, whether missing patches or configuration errors or something else, related to specific IP addresses. "We can scan 10 machines or 100,000 – daily," Austin says. The software identifies vulnerabilities and any exploits that have occurred. It will suggest repairs or restoration. It can also conduct penetration testing, that is, launch the exploit in a simulated fashion to show the nature and extent of potential damage.

"Most products are defensive in nature," Austin says. "We provide an offensive module that tests the network just as the bad guys would." To paraphrase a time-proven adage, a few meg of prevention is worth a gig of cure.

Smart Cards Optimize Info at Memorial Hospital in NH

The Memorial Hospital in North Conway, New Hampshire, had a problem, one common in the health care industry. It was running four different databases of patient information, and of course, none of them talked to each other. Wherever patients went, they had to re-register. They got annoyed. Hospital staff got less than perfect information. The error count crept up. Billing and payments slowed down. Just about every operation was affected.

The available solutions, short of starting over, were few, expensive, and complicated. Until Memorial encountered the LifeMed smart card. "We found we could overlay the smart card system, and it would talk to all four existing databases," says Lawrence Carbonaro, director of patient access. "Patients would register once, we'd have an audit trail for their information, and encryption and two-part authorization provided the security."

Memorial spent about a year installing the system. It set goals – among them, improve the quality of data, reduce the error date from 7 to 2 percent, and shorten reimbursement to fewer than 50 days. The new system went live April 1. So far, 4,000 cards have been issued to the hospital's potential patient universe of 20,000-25,000.

"Patients love it," Carbonaro says. "They register once, they swipe the card and they're good to go." The error rate on smart card-enabled accounts is already below 3 percent and falling. The hospital is making measurable progress toward all its goals.

Memorial plans over time to make LifeMed smart cards the center of its information system. "That's another beauty – you can start as small or as big as you want and grow," Carbonaro says.

MRC MERCHANT RISK COUNCIL

The Electronic Commerce industry is rapidly maturing – evidenced by:

- Consumer confidence levels are at an all-time high for online purchasing.
- Online sales continue to out-pace all other revenue channels for the vast majority of multi-channel merchants.
- The number of merchants falling under the umbrella of e-Commerce is steadily increasing.
- Online categories, industries, and vertical markets are rapidly expanding (social networking, digital downloads, and gaming among many others).

As an industry, we are seeing the traditional merchant challenges of fighting online fraud evolve into opportunities for new business models regarding data security and online payment strategies.

The Merchant Risk Council (MRC), a merchant-led trade association focused on electronic commerce risk and payments, is helping merchants identify and tackle these emerging growth issues that are unique to e-Commerce. The MRC provides industry stakeholders with special conference sessions, hosted webinars, regulatory change updates and reports on today's growing complexities of fraud, electronic payments, and online security.

The MRC has historically facilitated industry networking aimed at preventing online fraud. Today, our new education and advocacy programs are helping merchants succeed with their online payment, security and risk programs of tomorrow.

Tom Donlea, Executive Director, Merchant Risk Council

Southwest Airlines Cuts Fraud 50% with Accertify

There's always room for improvement. Southwest Airlines, one of the most successful companies in the history of the industry, enjoys an unprecedented string of 36 consecutive years of profitability. Its online fraud rate was consistently below industry norms, but with online bookings reaching nearly 80 percent in 2008 (southwest.com is the number one airline website for online revenue, according to PhoCusWright), management thought it could do better. It wanted a solution that was scalable, customizable, and leveraged new fraud-fighting technologies without affecting the airline's well-deserved reputation for customer service.

Southwest selected Accertify's Interceptas platform because it was the most comprehensive and flexible fraud-prevention platform in the industry. Interceptas was implemented in June 2008, providing a workbench platform that integrated all of the best-practice tools and key components required for a complete fraud prevention program. Implementation was quick and simple. Robust data management enabled Southwest to access 30 times more data in its screening process. The increase in available data paved the way for applying new business rules. The new platform streamlined a cumbersome manual review process and eliminated the need to use the passenger reservation system and other internal systems for reviews. A simple point-and-click process enabled Southwest to completely customize the user interface in less than a day. The integrated nature of Interceptas has also facilitated transaction resolution and chargeback processing.

The result? A significant reduction in fraud, leading to real bottom-line savings. Interceptas has provided Southwest with a clear return on investment. Four months after implementation (the company's normal chargeback cycle), Southwest saw a 50 percent reduction in its fraud rate as a percentage of sales, and in revenue losses due to fraud. Since then, the fraud rate has continued to decline.

New Tools Give Companies the Upper Hand in the Fight Against Online Fraud

It's a multi-billion-dollar problem the consumer rarely sees. But companies involved in e-commerce know all about it – they're footing the bill.

Online fraud. It cost U.S. retailers more than $4 billion last year alone. But the problem affects more than merchants. The anonymity of the Internet provides an easy environment for fraudsters to scam almost any type of organization, including airlines, hoteliers, government agencies, providers of digital downloads and multi-level marketing companies. Social networks have become targets for international con artists who misrepresent their identities to steal from other users.

According to Michael Long, chief product strategist at Accertify, Inc., reining in fraud can have an immediate and long-lasting impact on the bottom line. Long and his fellow founders worked in the online travel industry so they designed Accertify's software from a merchant's point of view. "Accertify offers the first end-to-end application to manage e-merchant risk," Long says. "Previously, clients had to establish relationships with multiple vendors, which was cumbersome and inefficient. We offer a fully integrated platform that focuses on work-flow and closes the gaps fraudsters slip through."

According to Long, the importance of data management is often overlooked in combating fraud. Companies typically keep data from customer profiles, registrations, purchases, merchandise returns and historical transactions stored in different places, files and formats. Analyzing and importing all this data into the prevention process is key to preventing all types of fraud, from retail crime to social scams.

"Companies need to strengthen their defenses by getting control of their data and using more automation and new technologies in their fraud prevention programs," Long says. "By choosing a solution that is designed to be flexible and integrates multiple fraud-fighting processes and tools, they will see a reduction in fraud losses more quickly and be able to adapt to new fraud schemes as they occur."

Accertify has worked with Southwest Airlines to reduce its online fraud rate by 50 percent in four months. Other clients include Urban Outfitters, Tickets.com and 1-800-FLOWERS.COM.

Long points out that the real cost of online fraud goes beyond disputed orders and chargeback penalties. Manual order review is expensive and slows customer service.

'Smart' Solution for Health Care IT Modernization

The need to bring the health care industry's information systems into the 21st century is well known. President Obama recently earmarked $18 billion to drive the process forward. What's perhaps less well appreciated is that the technology required to put health care records online in a simple, secure and accountable manner already exists.

Smart cards – plastic cards embedded with microprocessors – address several of the critical issues facing the health care industry, according to Randy Vanderhoof, executive director of the Smart Card Alliance. "Smart cards can capture patient information electronically – eliminating 90 percent of the paperwork – and make it available to those who need it while keeping it secure from those who don't," Vanderhoof says. "Imagine not having to fill out the same form every time you go to the doctor or the hospital. That's just the beginning of what smart cards can do."

Smart cards use sophisticated encryption and two-part authentication to give patients control over who has access to their personal information. They provide an audit trail, recording who has added or changed information. By authenticating the patient and the insurer, they can cut down on medical fraud. And the software behind them can talk to multiple databases, making medical information truly portable. "Think of it as a secure, portable database with translating capabilities," says David Batchelor, CEO of LifeMed Card, Inc., a supplier of smart card solutions to the health care industry. "It gives patients control over their health care information, and it starts building toward 100 percent accurate and complete medical records."

"Smart card technology has been around for years, it's proven," Vanderhoof says, pointing to employee and government ID cards as examples. "Smart cards provide a secure identity platform when they start architecting the new health care IT systems."

Ask the Information Security Experts

Darrell Covell, Founder/CTO Rsignia, Inc

What do you believe is the biggest threat in Cyber Security today?

First, acknowledge the reality of cyber terrorism. Stop hiding behind politically correct/safe terms such as "cyber security" and expose it for what it really is: Cyber Warfare! Russian cybergangs successfully shut down Georgia's entire infrastructure. We cannot delay implementation of cyber offensive capabilities. As we move to 10GigE, upward of 40GigE we need technologies that support such. Second, we need to expose vulnerabilities as these come not only from the outside but also from within. Rsignia has offensive cyber solutions available today providing sophisticated engineered solutions to these vulnerabilities. Exposing vulnerabilities without a solution is irresponsible. Rsignia works closely with the intel community as our engineers address current cyber warfare issues such as ID spoofing, location attribution, fibre tapping, sonet capture, layer correlations, IDS with GUI interfaces that utilize current open source solutions. These are new offensive cyber warfare solutions, where the old toolsets cannot keep up. We need an aggressive forward thinking stance.

Paul Sop, Chief Technology Officer, Prolexic Technologies

What does the future of cyber-warfare, and more specifically cyber-defense, look like?

A couple of trends are at work. The attackers keep getting more sophisticated. They've gone up against most of the commercially available technological defenses, and attackers know what they're dealing with. Attackers increasingly work for sponsors. They keep launching attacks as long as their sponsor pays them. This means it will keep getting harder to put the actual attackers in jail, and we are still left with the problem of how to defend against their attacks. Fundamentally, we have to engage the bad guys in the cloud, on the Internet, before their attacks get near their victims. Fighting these attacks requires much more than technology. You need battle-hardened pros, real people who've analyzed all the different styles of attacks out there, people who very likely can recognize who they're going up against. Victory today is making the attacker lose interest. That's more and more a matter of psychology and technology. There's no panacea. As the attacks get more customized, the defenses have to respond in kind.

Jeffrey Liesendahl, Chief Executive Officer, Accertify

What trends are you seeing in online fraud prevention?

Cybercrime is a global problem. Criminals are increasingly organized and sophisticated in using false identities to steal money and goods via the web. So retailers, government agencies and other organizations doing business online have to be more proactive in protecting themselves and their customers, especially in the current economic environment. Companies are doing everything possible to improve the online experience for consumers and maximize e-commerce revenues. But they also have to make more efficient use of limited resources and eliminate operational costs. They are focused on initiatives with a quick return on investment. Online fraud prevention is a critical area to address because companies can achieve results almost immediately. It's about more than cutting fraud losses and fraud-related customer complaints. It's also about increasing accuracy, efficiency and productivity of fraud-fighting efforts so the issue doesn't damage profitability, expansion plans or brand reputation.

Dan DeBlasio, Director of Business Development, Identity and Access Management (IAM) Americas, HID Global

How does "Risk-appropriate" authentication increase the value of security in an organization?

The usernames and passwords that organizations use to protect their computers and networks are too easily guessed, shared or stolen. "Strong Authentication," which requires devices such as a smart card or a one-time password generation token, increases security, but has been expensive. With "Risk-appropriate" authentication, businesses use a blend of technologies based on the location of their users and the value of the information protected. Frequent travelers might use smart cards, while their office-based colleagues would use their physical access badges, along with a personal identification number (PIN), to access their PCs. This "convergence" of physical and logical access is gaining popularity as it allows business to comply with industry IT security regulations using assets that have already been paid for. With this approach, the overall level of security in an organization is increased, while technology investments are appropriately controlled.

Dale Grogan, Director of Smart Card Initiatives for LifeMed Card, Inc

How can smart cards improve security in healthcare?

A patient's healthcare information is stored everywhere – at hospitals, physicians' offices, pharmacies, insurance companies – the list goes on. Unfortunately, this sensitive medical information is susceptible to theft; one of the fastest growing segments of identity theft is medical information. Thus, protecting medical information is vital. Data on smart cards are heavily encrypted, provide accurate identity confirmation, and act as a secure entry point for medical retrieval from multiple sources. As medical records become more widely distributed, (vis a vis President Obama's $18 billion initiative to fund Health Information Exchanges) the need to accurately identify and track patients, persons contributing patient information, and users of that medical information becomes more crucial. The point: smart cards help ensure patient medical record security and have been proven to be an unparalleled portable medical record device that provides accurate patient identity, reduces fraud, while streamlining patient registration.