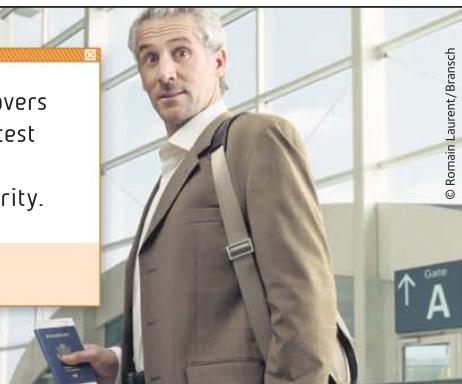


NOVEMBER 25 2008



Paul, 45, discovers he is the greatest innovation in digital security.



© Romain Laurent/Bransch

Digital security solutions for people who buy, surf, call and travel.

When Paul travels the world with his electronic passport, his only worry should be how to get to the airport on time. At Gemalto, we understand that protecting people like Paul in today's digital world begins with securing his identity and personal data. That's why our digital security solutions such as SIM cards, tokens, e-passports, banking cards, among others, are specifically designed for people like Paul and also fit in their pocket. This way he can fully enjoy his digital life while actively securing it.

[www.gemalto.com/digitalsecurity](http://www.gemalto.com/digitalsecurity)

**gemalto**  
security to be free

# MEDIA PLANET

## CONTENTS

Foreword	2
Turn Strategy into Action: Prioritize and Train	3
Balancing Risk is Common Sense	3
Know the Threat and Stay Competitive	5
The Facts and Figures of Security	6-7
New Storage methods bring New Risks	8
Holistic Approach to Combat ID Theft	9
Panel of Experts	11
Staying Ahead of the Game	11

## INFORMATION SECURITY A TITLE FROM MEDIAPLANET

Publisher: Annabelle Bernard,  
+1 646 922 1404,  
annabelle.bernard@mediaplanet.com

Editor: Sean Hargrave  
Design: Jez MacBean

Print: 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 contact the Director of Business Development at +1 646 922 1412 philip.thunstrom@mediaplanet.com

About this section: This special advertising section was written by Mediaplanet in conjunction with the advertising department of The Washington Post and did not involve the news or editorial departments of The Post.

www.mediaplanet.com

# A time for resolve



**Professor Howard A. Schmidt,**  
**President of the Information**  
**Security Forum (ISF)**

Until recently, information security was seen as a technical problem. Today it is a business imperative and should be on the top of boardroom agendas in every corporation and government agency. Information security can only be solved through a combination of technology, business processes, education and training and greater involvement of qualified information security professionals in business strategy and planning.

Information security is a moving target and there have been significant changes in the threat horizon. A recent ISF report shows that organised, profit-driven attacks are replacing random individual hacker attacks targeted at critical, core business applications and data repositories. Cybercrime is the fastest grow-

Risk is a word we use a lot these days and it has different interpretations depending on our experiences and context. When we talk about risk, we include dependency and over the last 20 years our dependency on IT and communications systems (ICT), has grown exponentially. This has led to a fundamental change in the information security landscape for personal, business and national security and the challenge to protect the integrity of data and critical systems is a primary concern at the highest levels.

ing type of crime and considered by the US Treasury to have exceeded the profits from illicit drug sales.

Another growing threat is from the proliferation of sophisticated mobile devices that are starting to replace PCs as the primary access point to ICT systems. With our dependencies on ICT systems, there is higher potential for designed-for-mobile malware such as Trojans and key stroke loggers; and we need to apply lessons learned in the desktop environment to avoid these devices presenting new 'back doors' for criminals.

While some Governments and Regulators look to address information security through more legislation and demands for greater governance this is only part of a solution. While these initiatives are well intentioned, the pressure for compliance can divert attention and investment away from solving some of the real practical risks.

### NEED FOR VIGILANCE

The recent financial crisis and today's uncertain business environment mean that corporations and their security professionals need to be even more vigilant. Now is the time to strengthen security rather than reduce it, which would expose us to increased exploitation. We all have to do our part to secure our part of CyberSpace.

Organisations such as the ISF play a role in this process by harnessing expertise and knowledge from organisations across the world to develop and deliver best practice to achieve a common goal.

*Professor Howard A. Schmidt is President of the Information Security Forum (www.securityforum.org). Howard has served as VP/CISO at eBay and as chief security officer at Microsoft Corp. Howard A. Schmidt was also special advisor for cyberspace security to the White House.*



Intersections Inc. (NASDAQ:INTX) is a leading global provider of consumer and corporate identity risk management services. Its premier identity theft, privacy, and consumer solutions safeguard more than 8 million consumers under arrangements with major financial institutions and under its own brand, Identity Guard®. To help combat corporate fraud, Intersections provides cutting edge identity risk management solutions.



Visit [www.gemalto.com](http://www.gemalto.com) to see how governments, wireless operators, banks, enterprises and more than one billion people worldwide use Gemalto's secure personal devices such as SIMs in mobile phones, smart bankcards, e-passports, identity credentials and USB tokens for online identity protection.



The Security Division of EMC

RSA is the premier provider of security solutions for business acceleration. As the chosen security partner of more than 90 percent of the Fortune 500 and many of our nation's national security and law enforcement agencies, RSA helps the world's leading organizations succeed by solving their most complex and sensitive security challenges.



ESET is a global provider of security software solutions for businesses and consumers. The award-winning ESET NOD32 antivirus product is recognized for providing superior protection from all types of malware. With offices in San Diego, California and Bratislava, Slovakia, ESET products protect over 40 million systems around the world. HYPERLINK "<http://www.eset.com>"www.eset.com



Conference & Expo

## The IT Security Event You Need is in December

Arm yourself with industry leader's insights. Build your cybersecurity defenses, network with peers, meet leading vendors, receive special hotel rates and use free transport from Penn Station.

All in New York City this December. Register today at [scworldcongress.com](http://scworldcongress.com) or call 877-418-4861.

Dec 9-10 | Javits Center | New York City

Speakers include:

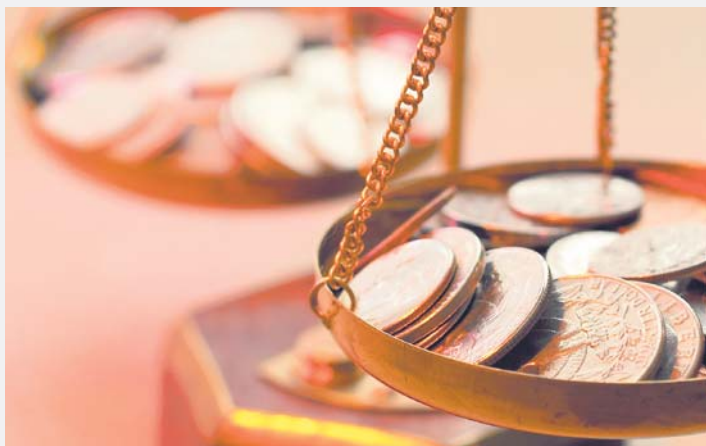
Congressman  
Jim Langevin  
(D-R.I.) ▼



Karen Evans, ▲  
administrator of  
e-government  
and IT, OMB

Louis Freeh,  
Former Director,  
FBI ▼





## Balancing risk is common sense

**A**lthough security spending is up, as a proportion of total IT expenditure, the fundamental problem facing information security executives is that for too long, experts believe, budget and risk have not been well aligned.

As Art Coviello, President of RSA points out, IDC figures show the 1% of IT budget spent on security in 2001 had risen to 3% by 2006 and is forecast to hit 5% in 2009. However, as Art states, "looking back to 2001, who actually feels three of four times more protected right now?"

The trouble is most companies roll out security networks without first considering risk. Without first prioritizing what is most important to the company there is a natural tendency to protect the majority of information moderately well and leave some unprotected.

"If you protect 90% of your information really well, chances are there's going to be some sensitive data in the remaining 10%," Coviello outlines.

"So companies need to work with a security company which can help them categorize the information they have and then they can prioritize putting their budget where the risk is, on the most sensitive information. It's common sense. If you were to look at my desk and I had a newspaper there, a competitor cost analysis report and legal documents for a merger, as you would imagine, I'm not bothered about the paper, I'd rather people not see the comparison, but I could live with it. The document I really don't want to leak is the merger details."

When risk is assessed in this way and categories assigned, it then allows a company to set policy rules which limits who has access to certain files and applies rules on whether it can be printed, emailed or copied.

Assessing risk, as a starting point, and then building a security response accordingly is a methodology which Eric Greenberg Senior Technology Consultant at Integralis believes enables companies to establish what they are getting for the security budget.

"The security industry doesn't normally talk about return on investment so we actually articulate the risk a company faces and put monetary terms on it so they can see where their priorities should be," he explains. "No security consultant can make all threats instantly go away, but you can work out the likelihood of a certain type of breach and its wider cost so you can figure out where the company can get its greatest return on security investment, based around risk mitigation."

# Turn strategy into action: Prioritize and train

**In an ideal world security would simply be a case of a strategist telling the board about the risks the company, its staff and customers face and then commissioning the necessary work to make the business as safe and compliant as possible.**

**H**owever, particularly in the current economic climate, budgets are tight and so bridging the gap between strategy and action requires a great deal of prioritizing and finding the right balance for a business between what it would ideally like to do and what it can afford.

As Gordon Rapkin, CEO of Protegrity points out, there is little appetite in corporate America for massive, expensive programs. What executives want to hear is priorities.

"There's just no point a security expert going in to a company and telling them they need to buy lots of new security systems because they just can't afford it all in one go," he says.

"Companies need to be given priorities. So my advice to a company is to map where its data flows. Normally there are stores of data in different places that are secure, say different offices or a brand's stores and its headquarters. It's likely that the data centers are protected to some degree but it's the path in and out of these data warehouses that are less protected. The bad guys are really good at finding weak points in a system, so where the data leaves one warehouse and where it enters another are the best places to focus on first. It's better to do that than to try to do everything all at once."

### SAFE STAFF KEY

Neville Patterson, VP of Government Affairs and Business Development at Gemalto believes that companies are now realizing that information security is an area they ignore at their peril. However, he believes some companies still have far

to go in turning strategy devised in the board room into action because they forget about the most important element within that company – its employees.

"Obviously if companies were writing blank checks there would be no end to what they could do but they obviously have to prioritize," he says.

"They need to understand where their risk lies and how this impacts their ability to secure their information and the information belonging to clients and customers. This can only be done if they engage in training their staff to adhere to safe information policies. A strategy that leads to new systems being installed needs the people operating those systems to be safe as well.

"It can be simple things such as training people never to leave the office with information on a USB memory stick unless it's encrypted and always making sure any information that leaves the company is digitally signed and encrypted. Most importantly, employees need to be given two factor authentication so they don't just log on with a password, but need a smart card or device or some kind or maybe a biometric, such as a finger print."

Likewise Randy Abrams, Director of Technical Education at Eset points out that companies need to provide the latest in anti-malware software as well as train to be careful online. In his experience many problems occur when staff inadvertently allow computers at home to become infected. Hence a strategy to get more secure in the office is not going to be effective, in his mind, unless staff laptops and their home office PCs are kept secure.

"You need to ensure the computers staff are logging in to your network from remotely are secure because they can provide a pathway in to your corporate network," he warns.

"Unless staff have got the same level of protection at home as they have in the office they might attract a piece of malware, such as a keylogger which can spy on the passwords they use and so give a criminal access to your systems."

It is for this reason that many security executives would advise companies to block peer to peer web services which are often used by people to illegally swap music and video files. These files not only often contain viruses but they provide a route through which a hacker can potentially gain access to a PC. Again, while these services can be blocked in the office, companies need to rely on training staff to understand the risk they pose and ensure they are never downloaded on to a computer they work on.



# Black Hat DC 2009 Briefings & Training

February 16-19 • Hyatt Regency Crystal City • Arlington, Virginia

Black Hat is the world's leading security conference focused on the needs of information security professionals.

[www.blackhat.com](http://www.blackhat.com)



# Can security answer the call to innovate?

## Global 1000 Security Executives Prescribe Risk/Reward Strategies for Innovation Success

In the past decade, the way business is conducted has shifted dramatically. Technology has allowed organizations to achieve levels of agility and productivity that few of us could have imagined. But, this progress has come at a steep price. The sheer volume, complexity and pace of our labors have substantially increased our overall business risk.

Organizations worldwide are struggling to gain a consolidated view of these escalating risks, which span every facet of the financial, legal, compliance, operational and market value chain. The sense of urgency is unprecedented. But sadly, most approaches to risk management have failed to evolve as quickly as the changing nature of business and government. And this is leaving many organizations flat footed in the face of a broadening economic crisis and unprecedented cyber-crime concerns.

### INNOVATION ESSENTIAL TO ECONOMIC RECOVERY

Many experts believe that the way out of our current financial turmoil will be innovation.

New products, services and business models are critical fuel for our economy. In the quest for market recovery and reassured confidence, it is essential that organizations do not shy away from business innovation. Fear of failure, or of running up against stricter and stricter regula-

tions, cannot be an excuse to step back from the call to innovate. If innovation is the path forward, it is more essential than ever to adapt to the changing nature of risk.

Whether it's on the massive scale of our struggling financial markets, or the more modest scale of most industries, organizations must learn how to master the risk-reward equation.

Information security leaders have a critical role to play in defining a modern approach to risk management, and setting a new standard for their organizations and industries to follow. They are in the best position to champion a progressive approach to information security that enables business innovation rather than inhibiting it.

*"Typically in most global organizations security is viewed at best as a necessary evil and more commonly, as a necessary friction. This derives from security's primary focus on attempting to constrain behavior to prevent negative events. Although well-intentioned, the inevitable result is that security practitioners are not viewed as enablers, but people preventing the business from doing what it needs to do."*

*Bill Boni, Corporate Vice President Information Security and Protection, Motorola*

### SECURITY EXPERTS WEIGH IN

Dedicated to reversing this tide, the Security for Business Innovation Council – convened by RSA – includes ten senior security, risk and privacy executives that represent some of the top minds in information security worldwide. This group shared their approaches and prescriptive advice on how to define winning risk management strategies in the recently published report, "Mastering the Risk/Reward Equation: Optimizing Information Risks while Maximizing Business Innovation Rewards." This study explores why legacy methods of evaluating information security risk don't work in today's connected

world, in which any new business innovation inherently carries some level of risk to information. In this landscape, the security focus must move from solely mitigating risk to also maximizing business reward.

*"Risk/reward decisions are business decisions. Not security decisions. So the business has to be involved and there have to be baseline policies in place that follow a standardized way to make the determination."*

*Roland Cloutier, Vice President, Chief Security Officer, EMC Corporation*

In an ideal world the risk/reward equation would be based on hard numbers. But realistically, it's not always possible. Many organizations use high, medium, and low risk definitions to describe probabilities and impact, or they use a numerical scale that assigns risk scores to qualitative

measures. Others make comparisons to identify the risks they believe to be relatively higher than others. The key is to arrive at a standardized way to view risk across the organization and apply it consistently.

### NEW MODELS FUEL BUSINESS VALUE

Beyond evaluating risk, another key priority is to determine who can make risk decisions. A risk assumption model as shown below formalizes risk decision-making authority across the organization. To effectively manage information risks for business innovation on an ongoing basis, a governance structure must also be in place.

This ensures that the effort is sustainable. An enterprise risk committee (ERC) can play a critical role, governing the overall risk/reward calculation process within the enterprise.

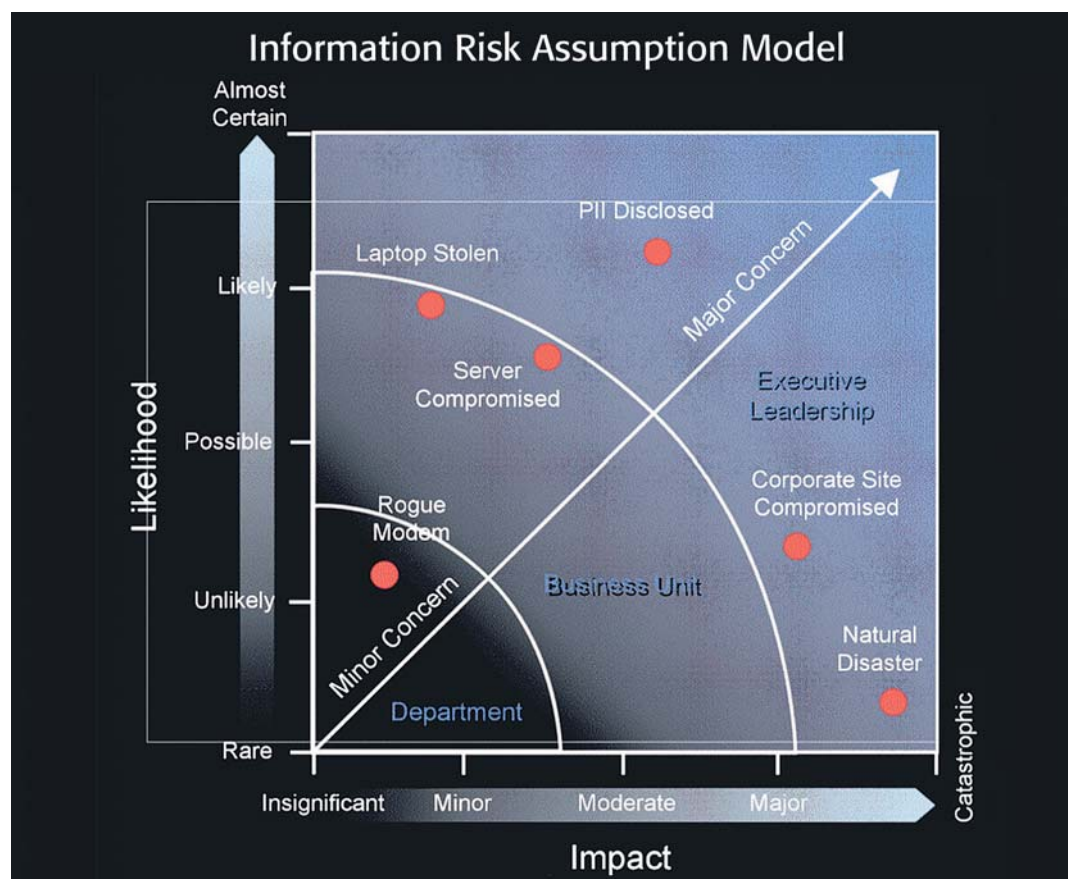
The RSA-sponsored report "Mastering the Risk/Reward Equation" includes many more proven Council strategies for making risk/reward calculations that drive business value, increase customer confidence and drive efficiency in government initiatives. This is an essential roadmap for any information security leader who wants to expand and transform their role from being a defensive protector of corporate and government assets to being a full partner in business innovation.

#### SECURITY FOR BUSINESS INNOVATION COUNCIL MEMBERS

- Anish Bhimani, Managing Director, IT Risk Management, JP Morgan Chase
- Bill Boni, Corporate VP, Information Security and Protection, Motorola
- Roland Cloutier, Vice President, CSO, EMC Corporation
- Dave Cullinane, Vice President and CISO, eBay
- Dr. Paul Dorey, Vice President, Digital Security and CISO, BP
- Renee Guttmann, VP, Information Security & Privacy, Time Warner
- David Kent, Vice President, Security, Genzyme
- Dr. Claudia Natanson, CISO, Diageo
- Craig Shumard, CISO, Cigna Corporation
- Andreas Wuchner, Head IT Risk Management, Security & Compliance, Novartis



▲ You can download a complete copy of this report, as well as the Council's first report "The Time is Now: Making Information Security Strategic to Business Innovation," by visiting [www.rsa.com/securityforinnovation](http://www.rsa.com/securityforinnovation).



A graphic representation of a risk assumption model might look something like this: various grades of risk decision authority - from department to business unit to enterprise to executive leadership - are mapped to several potential security events, which have certain likelihood and impact.

# Know the threat and stay competitive

**There was a time when the greatest risk to information security was teenagers eager to show off to their peers. Writing code which made machines crash or show odd messages was a joke which gained a misguided individual respect. However, today's threats come from a range of criminals who are motivated by money rather than respect from hackers.**

As Howard Schmidt, President of the International Security Forum (ISF) and former White House cybercrime advisor sums up, there are three main threats which can ruin a company's good reputation.

"You have opportunistic fraudsters and scammers who are pretty low tech and then you get informal groups of people who are a little more high tech and will join together for a project," he says.

"They don't normally go beyond phishing scams and 419 letters where you're asked to give someone your bank account details so they can get money out of Africa. The most serious threat comes from criminals who permanently work together and who are very smart and tend to also be in to drugs, guns and child pornography too. Rather than

make a loud bang and show that they are there, they are very adept at getting into a system and remaining unnoticed so they can leak out information over a period of time. They get far more sensitive data that way and so the saying, "if you've never found someone in your system, you probably haven't looked in the right place."

#### DAMAGED NAME

Of course, the trouble is, as a hacking organization takes money out of a business through deception, it leaves behind it a tarnished reputation. One need only think of the damage done to retailer TJX when cybercriminals managed to steal millions of customers' credit card details.

Hence, Richard Wang, Manager of

SophosLabs points out that security is one of those areas where it is very hard to talk about the competitive edge which safe systems give a business because, normally, the value they offer can only be measured in comparison to the damage caused by breaches elsewhere.

"You can't really say that good security gives you a competitive edge, although it obviously does, but what you can definitely say is that not having good security makes you uncompetitive," he says.

"It's just common sense. If you have been a customer of a business that gets breached and your credit card details are made available to criminals, are you going to be happy going back to that business, or would you feel safer using an alternative company?"

#### BRANDJACKING

This leads on to another issue which might not strictly be seen as part of a company's own information security strategy but can definitely lead to a deterioration in the brand's good name if they do not react to the threat.



It does not matter how well secured a company's data centers are and how well they handle customer and corporate information as it switches from one center to the next, if a brand has a recognizable name, online criminals will do their best to make an illicit living from it.

According to Frederick Felman, Chief Marketing Officer at brand protection security company, MarkMonitor, cyber criminals are getting increasingly adept at setting up sites that mimic a brand's appearance to lure in its customers and take payments for non-existent or fake products.

"I have known people from the brands themselves and people inside information security look at criminal sites and they've been astounded by how good they have become," he says.

"They're nearly always an extension of that company's brand name so it can

seem a natural place for people familiar with the brand to go. When they get there if they shop they can end up giving away their credit card details which are then used by the criminals. Often the person will get no goods or receive counterfeits.

"Even though it's criminals, and not the brand, who are ripping people off, this 'brandjacking' leaves a bad taste in the mouth of its victims and can really put people off going back and shopping with the real brand."

Hence Felman's advises companies use a system which allows them to check new and existing domain registrations for use of their name and trademarks because if left unchallenged cybercriminals can do untold damage to a brand's reputation and the first thing they know about the problem is disgruntled consumers clogging up their customer help lines.

## The End of Passwords: Digital Keys for Computers

**If you are a federal government or private sector employee, chances are you'll soon need a key to drive your computer.**

Not a metal key of course, a digital security key that will replace your password. But unlike passwords, this will be something you will physically carry and use to more safely identify you online.

Why? Because passwords alone just do not provide enough online protection to you as an individual, or to the organization you work for.

"Imagine you could withdraw money at an ATM by just entering a

PIN code. No ATM card required. Would you trust that?" asks Francois Lasnier, vice president and general manager, security, for Gemalto North America.

Lasnier argues that would mean that if someone could get your PIN code, say by filming you at a grocery store checkout, they could clean you out. But that is exactly what we have protecting most desktops and network access today—reliance only on passwords to identify you. Stealing

those passwords is the goal of online security threats like phishing and spyware. Even co-workers can be a threat.

All that is about to change. Lasnier's company, Gemalto, the world leader in digital security, is at the forefront of bringing a new and significantly safer way of protecting identities online.

The concept is simple: give people a personal, portable security device that is protected by a simple PIN code. You use this device, either a card or USB token, as a digital key to access your desktop, laptop or company network. Security pros call this two-factor authentication. It is also a lot more convenient than remem-

bering long, complicated passwords.

Washington D.C. is at the core of this network security revolution, according to Lasnier. Four million federal government employees already have either a PIV (Personal Identity Verification) card or the DoD Common Access Card (CAC) card. The DoD is already using these to provide secure logon, and other federal IT departments are readying their systems to use the PIV card for the same purpose.

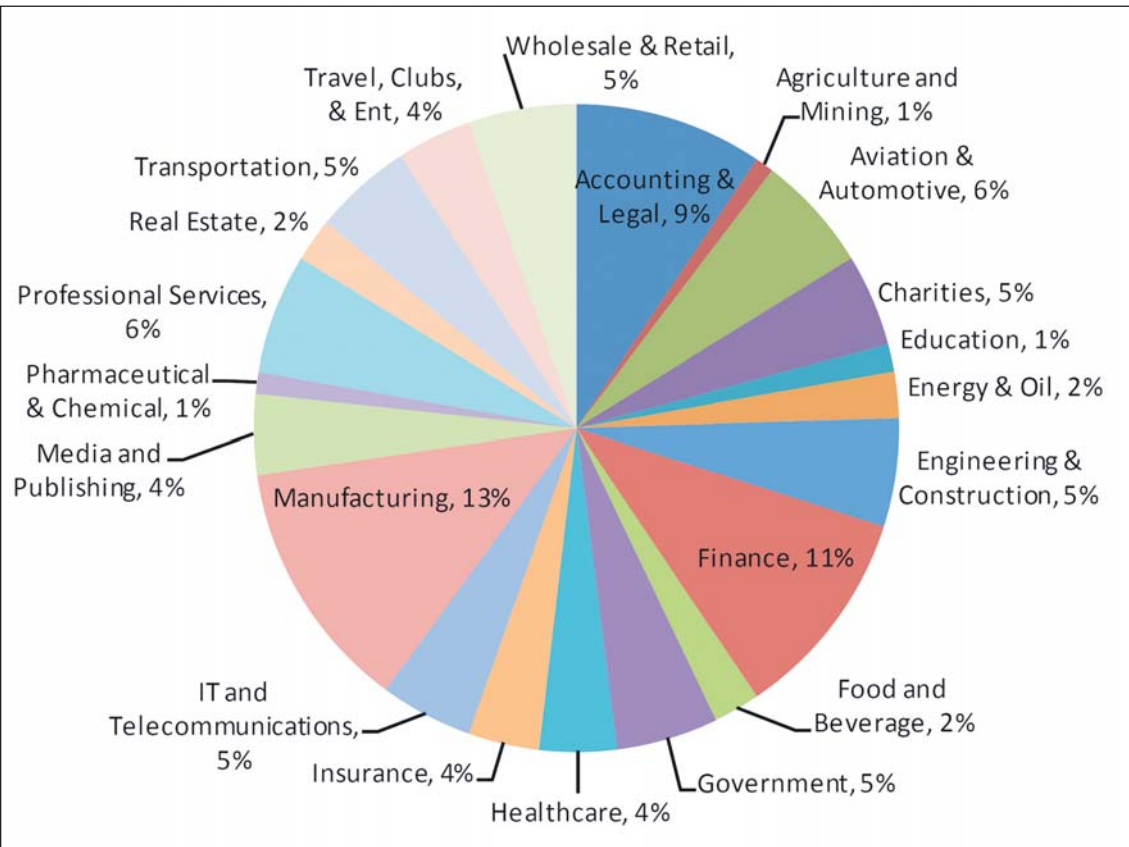
In the private sector, many blue chip companies including Pfizer, Boeing, Microsoft, Chevron, Caterpillar and many others have already implemented some form of smart card-based network security.

The underlying technology is a smart card, a small computer with its own software in a normal, credit card-sized plastic card or USB token. Today smart card technology protects more than two billion mobile phones and 730 million smart credit cards worldwide from fraud. Gemalto is the world's largest producer of these digital security devices for both mobile operators and banks.

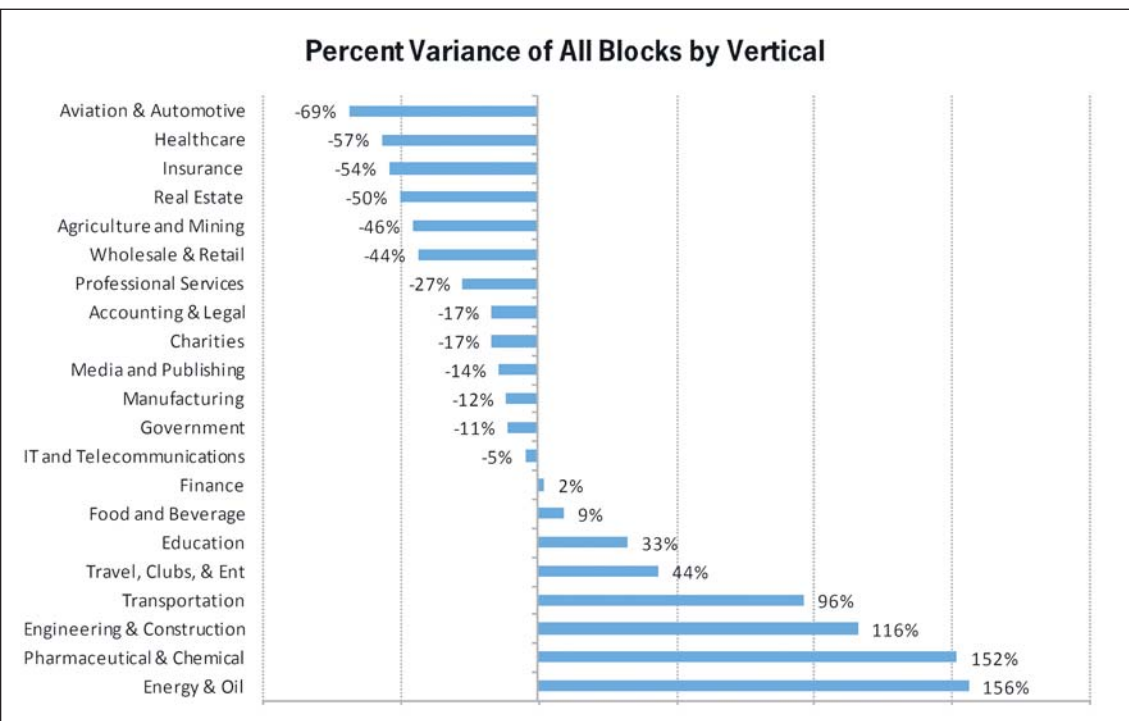
**Francois Lasnier, vice president and general manager, security, for Gemalto North America**

# Which industries are most at risk – and from what?

San Francisco-based ScanSafe monitored the web throughout the first three quarters of 2008 to see where malware attacks are aimed. They wanted to get a picture of which industries are more prone to attack than others.



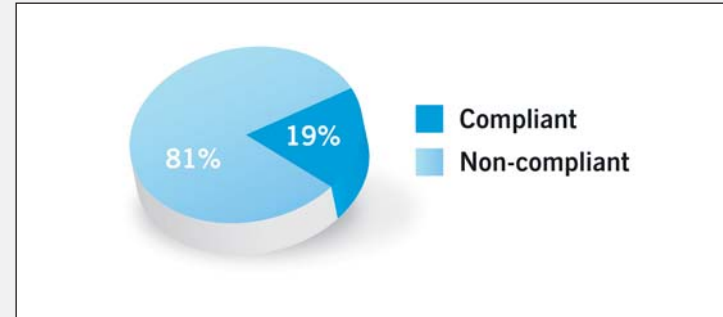
ScanSafe took a slice of the industries present on the web.



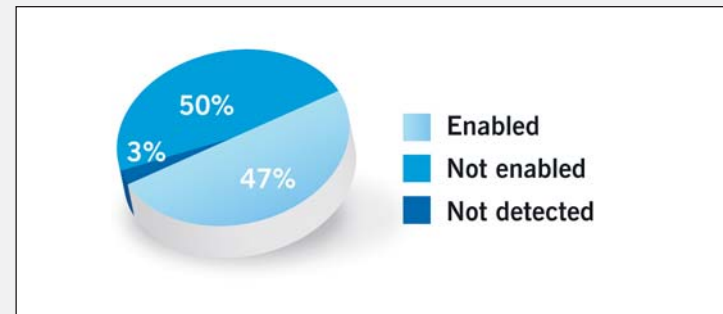
The researchers then averaged out then reduced each vertical to a level playing field so that an industry with more web sites than another did not seem to be more at risk, simply because it had companies operating more web sites. The results, then, show the total risk for each vertical. Here, 0 is the average and a minus shows fewer than average attacks, a positive result shows more than the average.

## So what openings are businesses leaving open to cyber criminals?

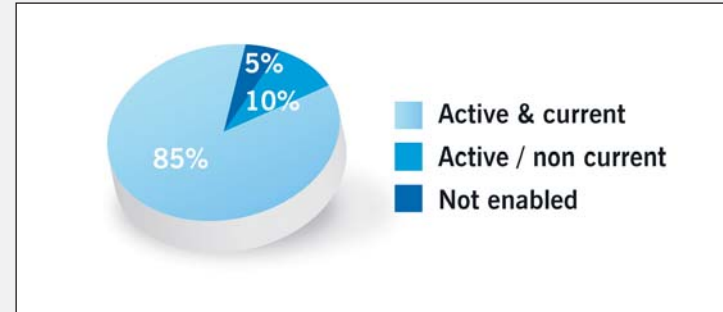
Four in five PCs are left unprotected against cyber criminals due to bad configuration and security software not being up to date.



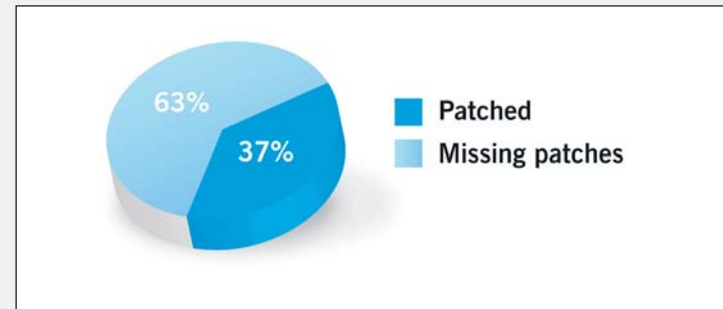
Boston-based IT security and control company Sophos offers a free 'endpoint security scanning service online which allows companies to find out where their potential weak points are. The company took a poll of 580 PCs scanned over a recent 40 day period to produce a picture of where American businesses and consumers are letting down their guard. It found that the vast majority of PCs were not as safe as they should be, either because their anti-malware software was not up to date, their firewall was not turned on or security patches for common computer programs were not up to date. The results found four in five American PCs are not 'compliant'.



Half of the country's PCs do not have working firewalls set up.



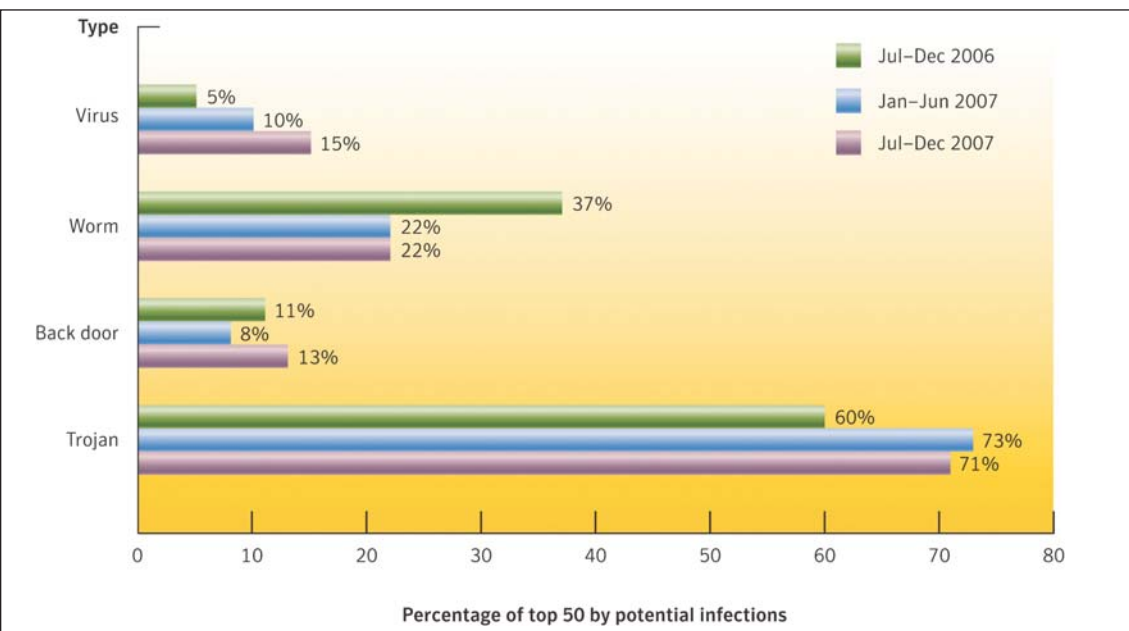
Anti-malware results were better, the vast majority of PCs were protected.



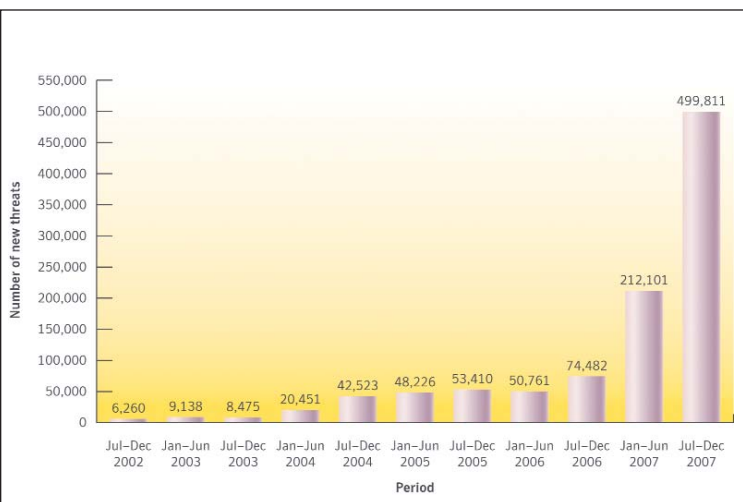
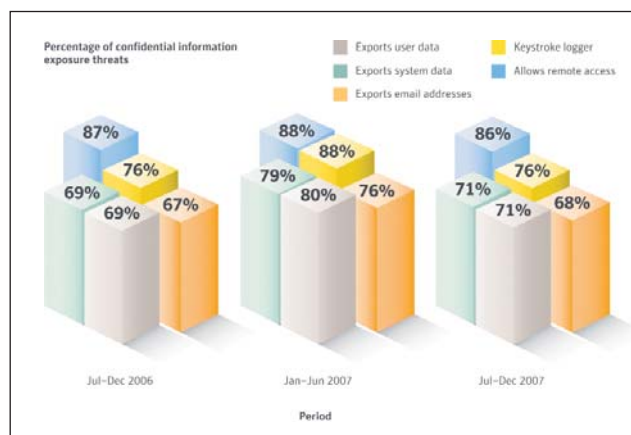
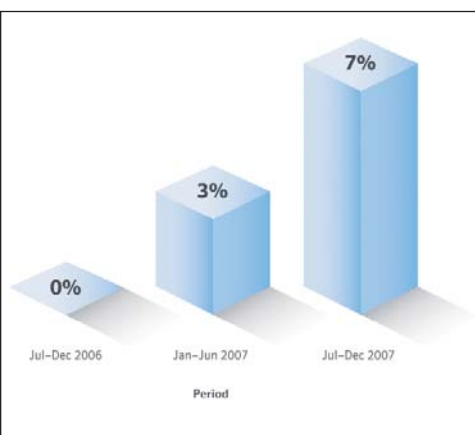
Security patches were a cause of concern, nearly two in three PCs were missing patches.

# Are information security threats growing? Where are they coming from?

Symantec's research has shown a significant increase in threats online but also shown that America is far and away the biggest target for phishing.



Viruses are on the increase but worms are less prevalent whilst Trojans are still the number one threat.



Above left: The proportion of overall malware which is designed to modify websites vastly increased during 2007.

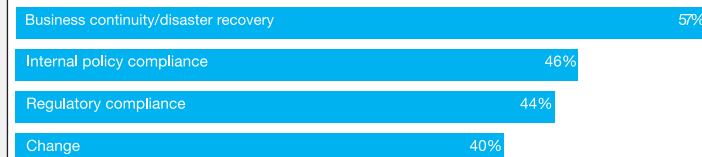
Above right: The relative threats to confidential information being exposed stayed relatively stable across 2006-2007.

Left: The number of new malicious threats seriously escalated at the end of 2007.

## How are these increased threats being handled by IT executives?

The Global State of Information Security Survey 2008 PricewaterhouseCoopers (PWC) asked 7,000 IT executives, CEOs and CIOs how they, their board, their company heads and business partners are dealing with heightened information security threats.

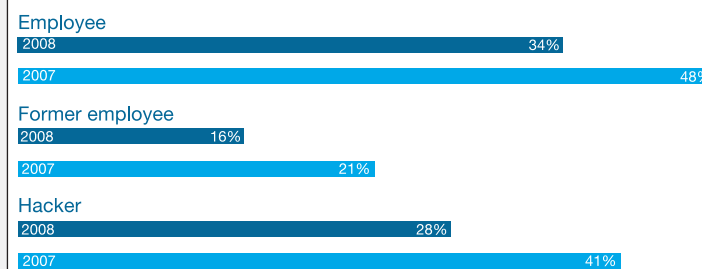
Percentage of respondents who identify the following business issues or factors as the most important drivers of information security spending in their organization



Percentage of respondents reporting gains in key processes and people-related capabilities



Estimated likely source of security incidents over the last 12 months



Few respondents are very confident in their partners' or suppliers' information security practices



# New storage methods bring new risks

Whilst the latest trends towards virtualization and 'cloud' computing may bring with it great cost savings and flexible working benefits, it does raise considerable security and legislative concerns.



The idea of cloud computing is particularly attractive to a small and medium enterprise. Many large companies will have their own data centers which are professionally managed by their own staff but, for a smaller company, the cost can be too great. Hence, uploading company information to a storage provider who keeps it in the 'cloud' from where it can be downloaded with the correct user name and password is an attractive, affordable solution.

## SARBANES-OXLEY

However, according to Kurt Roemer, Chief Security Strategist at Citrix there are many associated risks which he feels have not always been realized by customers. Most businesses are aware of Sarbanes-Oxley rules which require them to keep data logs so it always knows where data has been stored and who has accessed it, however, some states have additional laws about where data is stored and how.

"If you put your data up in to the cloud it can seem great that you're paying very little for storage," he says.

"However, you don't know where it is being stored, it's up there in the ether somewhere. There are states that require you know where your data is and that it hasn't crossed international boundaries. If you just upload to any cloud provider without checking, you could be breaking that law by having your customer data stored outside of where it should be."

Roemer also suggests that a simple user name and password are not sufficient and businesses really need to opt for a system which offers two factor authentication, where a token (often a

key ring fob) provides a variable password for the legitimate user. Encrypting information before it is uploaded to the cloud is also a good idea because this ensures it is encrypted to the company's standard and is scrambled on its route to the cloud and so cannot be intercepted.

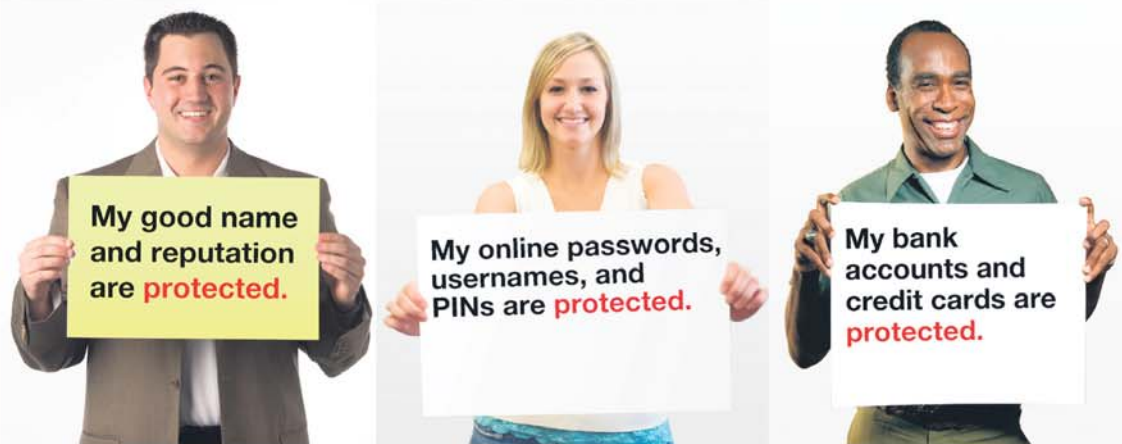
## DRIVE RULES

Whilst this is good advice for data stored beyond a company's offices, there are always new threats within its own four walls, warns David Vergara, Product Marketing Director of Endpoint Security at CheckPoint. While the iPod and USB memory disk (or 'thumb drive') may seem like wonderful gadgets, they can pose huge risk to data systems.

"Small drives are capable of holding so much information now that companies are finding out the hard way that a lot of their sensitive data can be downloaded and taken away by an employee," he warns.

## ENCRYPTION

"That's why I'd advise companies to investigate systems which encrypt all information on a hard disk so it can only be read on a machine that has the key to unlock it. They should also set up an administrator system which says which devices are allowed to connect to their computer system. With this they may set up all the employees machines to not accept an iPod or an external drive of any sort or they can specify the particular type of 'thumb' drive they will allow. They might, for example, want to allow the thumb drives the company issues but then block all other makes."



Protecting what matters most to you is what **matters most to us.**

**IDENTITY GUARD® Total Protection**  
now with ID Vault

Your passwords, screen names, and credit card numbers will be virtually impossible to steal when you're online.

Try **IDENTITY GUARD Total Protection**  
**Free for 30 days**

[www.identityguard.com](http://www.identityguard.com) | 1.800.452.2541



# Information assurance: Never-ending vigilance

**In today's data-centric world, information is king. Expectations by network users for timeliness, security and integrity of that information have never been higher. When the network is down, employees might as well go home. Dr. Ronda Henning, Sr. Scientist and Information Security Queen, Harris Corporation**

Unfortunately, most organizations take their network and the information shared via their network for granted. A network status of "available" is the only acceptable status, and complacency is never an option for the IT department.

Today's truly successful networks provide information assurance (IA) by delivering the right information, to the right person, at the right time.

But, the information is only as good as the environment and maintenance policies practiced by the organization that designs, delivers, and operates the network. Mission-critical networks are carefully engineered, implemented to exacting requirements, and tested to discover and correct potential problems.

An adversary has to find only one flaw to successfully attack...a de-

fender has to counter all adversaries. As threats continue to escalate, the complexity of security breaches is also increasing at an exponential rate. At the same time, security requirements are heightened by new government confidentiality regulations and increased personal mobility.

Assuring a network demands vigilance throughout the system's life cycle. The secure state of a network is a living, functioning system that must be preserved and protected once it is placed in operation. Maintenance of an assured network requires systematic installation of updates and continuous monitoring of security protections incorporated into the system.

Monthly updates will correct problems as they are identified, but only if

the network operators make the installation of these updates a priority. Vigilance must continue even at the end-of-life of a system. When a system is ready to be discarded, the storage media must be carefully examined to ensure sensitive information is not accidentally disclosed.

Harris Corporation, a world leader in Information Assurance, uses state-

of-the-art technology assessment techniques and architecture engineering to define and operate secure networks. Our technology countermeasures and monitoring proactively safeguard vital information assets for the U.S. military, the U.S. Census Bureau and the Federal Aviation Administration. Harris is serious about Information Assurance.



**On May 20, 2008, the Florida Institute of Technology broke ground on the Harris Center for Science and Engineering, a 27,000ft<sup>2</sup> facility dedicated to the advancement of computer science and information assurance.**

## Holistic approach to combat ID theft

**There are very few people that have never heard of identity fraud. With nuggets of personal information such as credit card details, a social security number or bank log in details, criminals can bleed accounts dry as well open up new lines of credit. When one identity's worth is exhausted, they simply move on to the next victim.**

Anybody impacted by identity theft will testify that it is far from the 'victimless' crime which its perpetrators label it to be. Although a victim does not have to go through the ordeal of being robbed face to face, they still have the ordeal of coming to terms with somebody having stolen their personal information and pretended to be them in order to defraud credit card companies, banks and stores.

More recently identity thieves have extended their fraud into providing false identity for illegal workers and for fellow criminals who commit crimes under their assumed identity, leaving a bemused victim having to explain their innocence to investigating police officers.

Perhaps most worryingly, identity thieves have started to use stolen personas to claim medical treatment for which they are not covered, not only defrauding the system but also running the risk of a victim's medical history being compromised.

Whatever the intent of the criminals, identity theft is more than a nuisance. It can make people feel violated, leaving them with no money and needing to take personal days off work to reinstate their good name with their bank, credit agency and the police.

### **MORE SOPHISTICATED**

For Michael Stanfield CEO and founder of Intersections Inc., the main problem with identity theft is that criminals are

no longer just relying on 'dumpster diving' or stealing wallets to gather personal information. Today's sophisticated identity thieves are becoming adept at launching viruses which can sit on computer hard drives stealing information and gathering sensitive passwords. Alternatively they can produce sophisticated sites which look like a bank or a regular store but are actually 'phishing' sites designed to gather credit card and bank account information for criminal use.

Hence, to Stanfield, the only way to offer protection against identity theft is to take a holistic approach.

"You can set up fraud alerts and credit card blocks so you won't be a victim, but a lot of identity theft doesn't come from credit card theft," he says.

"A lot of people are having their bank accounts drained by 'keylogging' software that sits on their computer and tells criminals what their passwords are. So, you can set up fraud alerts but they are not effective unless you secure the PC at home."

In addition to daily checks with the credit reference agencies, records of

new mobile phone accounts and details of social security or credit details being sold online, Stanfield argues ID theft protection companies should also offer anti-virus, anti-phishing and anti-spam protection on the PC as well as the ability to block 'keylogging' software.

The sad fact is that no matter how careful a person is in terms of securing their computer and shredding their personal information before it goes into the garbage, they can still become a victim of identity theft, or at least credit fraud, through no fault of their own.

Hackers are becoming increasingly adept at finding ways into corporate systems and stealing credit card details which are then normally sold online to other criminals. Gordon Rapkin, CEO of corporate information security company, Protegrity, believes many businesses need to look at their own data in a new light.

"You just have to look at all the cus-

tomers records you have and instead of seeing a line of data imagine it as anything between \$5 and \$100," he says.

"Then they need to think about how many of these they have and how many pass through their systems every day. There are thousands of these records that are worth between \$5 to \$100 on the criminal market flowing through their hands every day. They only then need think how much they pay the person handling that information to realize the temptations on staff and the need for them to secure systems so staff never see all the records and certainly can't record or copy it."

A few simple security procedures and policy rules regarding how they handle data could solve many leaks of customer information which can end up costing a brand its reputation as well as having to undergo the embarrassment, and expense, of continued annual audits of its systems by the FTC.



# Panel of experts



**What is going to be the impact of the economic downturn, in security terms?**

I see two main reactions. The main factor is there is inevitably going to be more regulation. At the same time people are going to

be cutting back on security spending, not that they want to cut back on security, but because they're cutting back on everything. The trouble is I can foresee this will have an adverse effect on innovation. I think there will be so much extra regulation around that people will become risk adverse and there will potentially be less budget available.

With a cut back in security spending people will be even less likely to take the kind of risk that innovation requires and security can enable. So the result is that business innovation could suffer, with organizations choosing to shut down key growth efforts out of fear rather than leveraging security technology to its full potential to make them happen. You have to remember, though, that security should still be a high priority because criminals will be still be as much, if not more, of a threat and you will have the extra problem of people being laid off and posing a potential threat to their former employees. So the risks are not going down, they're actually only going to increase.



**Against a tough business climate people are likely to cut back on security. What would you warn is the cost of complacency?**

*Randy Abrams, Director of Technical Education, Eset.*

Malware is obviously used to steal sensitive information and to find out passwords so criminals can perpetrate identity theft but it goes a lot deeper than that. There is the very real risk of a business having its intellectual property viewed by a competitor. There was a case of this in Israel where an automotive company found it had a Trojan on its system that had been leaking proprietary information to a rival. There's also the real risk of losing reputation if you have a security breach as well as your work computers being used by criminals as part of a 'botnet' sending out spam without your knowledge.

A problem people don't often realise is that criminals will often use malware to plant illegal material on a company's network so they're not caught with it themselves. It can obviously be very embarrassing and distressing when the cops come knocking on the door and you realise your corporate systems have been selling child pornography or illegal MP3s – how do you explain that to the police. The same problem can mean employees are wrongfully fired for having illegal material on their machines which they had no idea was there.



*Neville Patterson, VP of Government Affairs and Business Development, Gemalto.*

**How are changes in government policy impacting security in businesses?**

There is a huge trend at the moment for smart identity cards to be used as part of two factor authentication, which is a very positive step.

The Federal government is taking a real lead here with its Homeland Security Presidential Directive (HSPD 12) programme to issue identity cards to allow federal employees access to one another's buildings but also one another's computer systems. This is having a trickle down effect whereby if you are working with the government you need a smart identity card. We're now seeing something like 10,000 cards being issued to the Federal government every week, so it's a great case of government providing a proactive lead for industry to follow.

It's also very good news because it is bringing in standards to the market which were much needed. We're now seeing a lot of interest in companies following the lead and having their own cards which members of staff need to use as one part of a two factor logging in process, normally in addition to a password. Our suggestion has long been that companies go for two factor authentication because it is an extra level of security. It means a lost or stolen laptop is useless even if a third party knows the password and it ensures that people are who they say they are when they log on to the corporate network and aren't using someone else's password without their knowledge.



*Yuval Ben-Itzhak, CTO, Finjan Software.*

**What has been the major knock-on effect in information security in terms of the global economic downturn?**

There are two sides to this question; the cybercriminals and the CIOs. Both will be affected by the economic downturn. The more unemployed IT and software people there are, the more likely it is cybercrime will grow. We have seen this in the last year in Eastern Europe and Asia where unemployed system administrators and other IT people found an easy way to get money by conducting cybercrime. With the toolkits professional hackers are selling online, almost anyone with an IT background can start stealing credit cards and other valuable data almost instantly.

On the other hand, more cybercrime means, for CIOs, that more security is needed and improvements in TCO. Although budgets are becoming an issue, focusing on TCO and security technologies that focuses on today's cybercrime techniques fits the expected effect of an economic downturn perfectly. As for 2008, Finjan is not seeing any budget cuts in IT security yet. These budgets were already approved in 2007 and early 2008. However, 2009 budgets are still 'in the air'. IT security has a minimum cut and sometimes grows as a percent of the total IT budget that might itself be cut. In post-bubble slowdown IT security budget remained at the top of the list, above the line, while other budgets were affected. This behavior is cross verticals – IT managers understand the importance of security for their business to operate and succeed.

# Staying Ahead of the Game

**External threats to corporations tend to change from time to time as criminals find ways around defense systems but there is one common aspect to many information security threats, a hacker on the outside has to find their way to the inside and, like a real life burglar, they will normally look for an open door.**

It is for this reason that Sandy Weil, CEO of Proginet, which specializes in secure file transfers, believes the latest trend in information architecture holds a lot of promise.

"Companies want to do lots of 'handshakes' with customers and their own staff all day long, so you have to find a way of letting the good guys in and keeping out the bad guys," he surmises.

## DEMILITARIZED ZONE

"One way is to take a leaf out of military history and set up a DMZ around your networks. This demilitarized zone is, just like in real life, a no man's land. For information security it ensures you have two firewalls and so two barriers around your information. Trouble normally comes from allowing somebody an unbroken connection in to and out of your network so you instead allow

somebody in to the DMZ, break off the connection back to them and once they're in your border area you decide whether to let them in fully."

## EDUCATION KEY

Ultimately the way that businesses and individuals can best defend themselves is education, urges Alfred Huger, VP of Development at Symantec.

"You can put whatever systems you like in place within a business but it's nearly always user behavior at some point that will pose a problem," he says.

"You need to educate staff as to what is safe practice. They need to know about phishing and how to avoid obvious email scams. They need to keep computers' anti-virus up to date and they need to connect to the office from home on a secure connection because otherwise they could be giving away sensitive data or picking up malware on a laptop that they'll be bringing in to work the next time they're in the office."

## INFOSECURITY EUROPE 2009 – GATEWAY TO EUROPEAN MARKET

Infosecurity Europe is the No.1 industry event for information security with more than 12,000 visitors attending and 350 exhibitors, showcasing a diverse range of new and innovative products and services from the world's top information security suppliers. The event enables security professionals and business managers to establish a commercial justification for information security, refine their security policies and select the most appropriate solutions to support their security strategy. The unrivalled free education programme addresses both strategic and technical issues drawing on the skills and experience of senior end users, technical experts and real world case studies.

**Infosecurity Europe takes place at new venue, Earls Court, London, UK from 28th- 30th April 2009 - [www.infosec.co.uk](http://www.infosec.co.uk)**



# Protect Your Identity and Data During Tough Times

Each day worldwide economic headlines indicate more and more economies are under stress. History has shown that during economic downturns, criminal activity rises. Under these circumstances, the already alarming rise in online business and consumer data and identity theft can only be expected to increase.

According to IDC's Program Director of Security Products, Brian Burke, "The second most significant threat for business today is malware — trojans, rootkits and other malicious code — and both businesses and consumers are exposed to identity and data theft which is already costing the economy billions of dollars."

Burke adds that the challenge of avoiding attack has become increasingly difficult. "In the past," says Mr. Burke, "threats were made to be noisy and highly visible. Unfortunately, today's threats are often silent and often go unnoticed until the damage is done."

Unlike other endpoint security software, ESET's antivirus and malware software uses ThreatSense technology to identify and stop unknown attacks before they can cause damage. Instead of relying solely on "signatures" to spot known attacks, ESET software actually inspects any potentially dangerous file to identify suspicious behavior and block it, before damage can be done.

Anton Zajac, CEO of ESET stated, "We compete with a technically superior product that our customers trust and tell their friends about. No matter how many updates they ship per day, our competitors have not been able to match ESET's unrivalled combination of effective proactive protection and low system overhead."

Syndicated radio talk show host of the "TechGuy," Leo LaPorte agrees. He is a loyal user of the product and continues to evangelize it as the most effective endpoint protection on the market.

ESET's products are now in use by over 70 million users around the world and are available in over 160 countries. Find out more at: [www.eset.com/post](http://www.eset.com/post)



If you use Windows, you need my favorite antivirus — ESET NOD32.

Leo LaPorte



THE SMARTEST IT MANAGERS  
DON'T MAKE PROBLEMS GO AWAY.  
THEY MAKE SURE THEY NEVER APPEAR.



**ESET®  
NOD32®  
Antivirus**  
Business Edition



**ESET®  
Smart  
Security™**  
Business Edition

Proactive + Precise + Lightweight + Fast



[www.eset.com/post](http://www.eset.com/post)

© 2008 ESET, LLC. All rights reserved. Trademarks used herein are trademarks or registered trademarks of ESET in the United States and certain other jurisdictions.

**“I am fearless.**

I secure identities and information  
for a major federal agency.

I offer citizens confidence  
in the online channel.

I lead.

I innovate.

I win.

I am fearless.”



When it comes to security, most organizations understand what it means to fail. But few can imagine what it would mean to succeed. RSA's information-centric security solutions can move your agency forward to address the cyber threats of today and tomorrow. That's why we're the chosen security partner for key defense, intelligence and other leading federal agencies. Fear less. Do more.

Learn more at [www.rsa.com](http://www.rsa.com)



The Security Division of EMC

Secure Anytime  
Anywhere Access

Protect  
Customer Identities

Secure  
Enterprise Data

Manage Compliance  
and Security Information