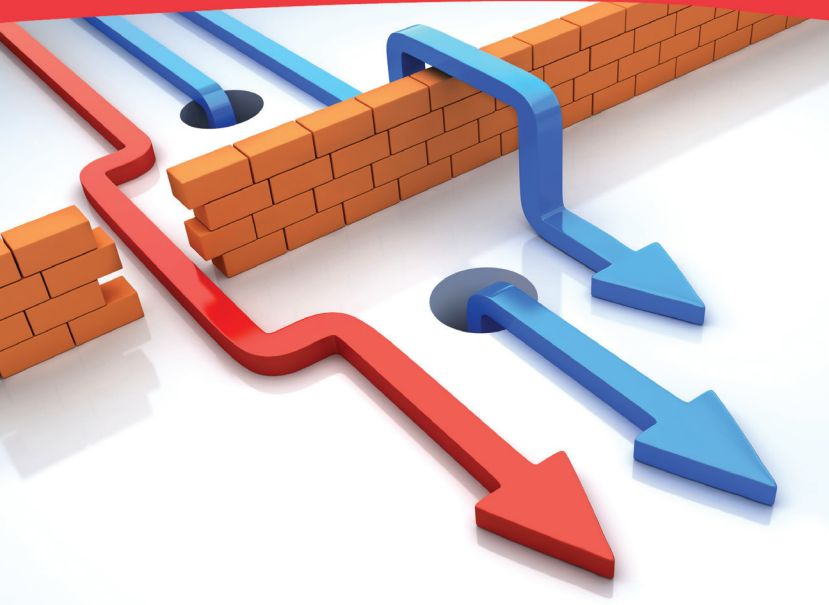
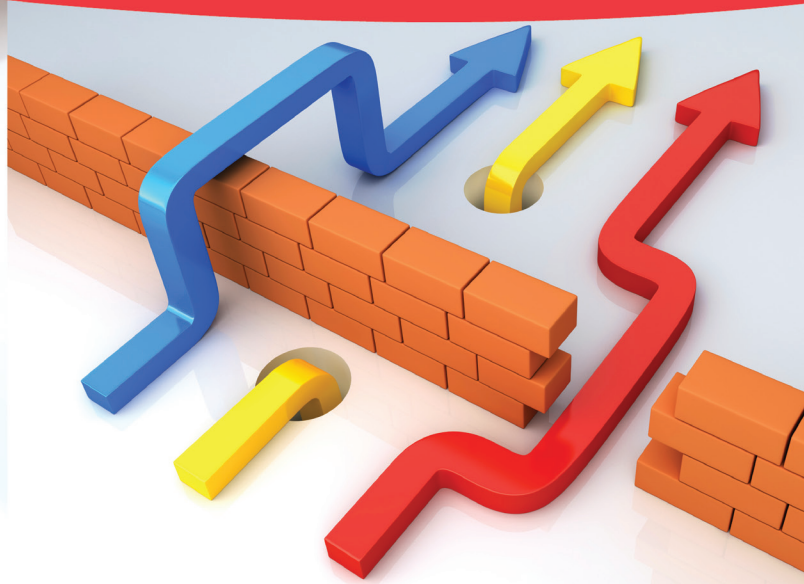


An InDorse Technologies Security Whitepaper

Securing Data During Hard Times

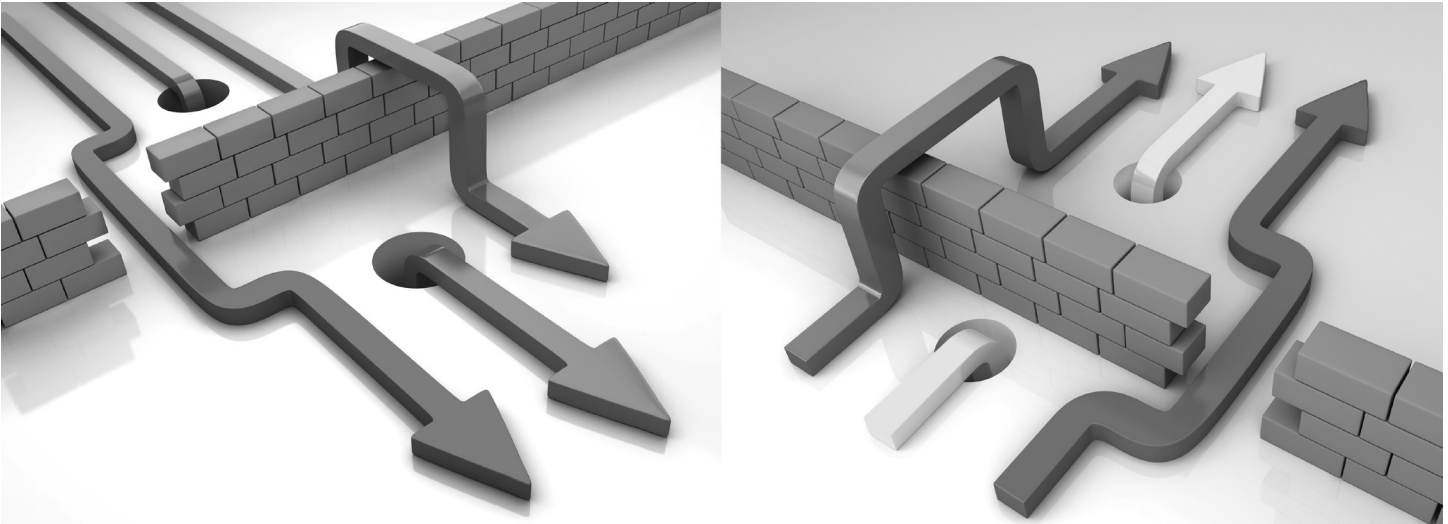


bad stuff coming in



good stuff leaking out





Abstract:

This whitepaper analyzes the cost-benefits of protecting corporate data during the tough economic times of 2009 & 2010. These are the times that require “doing more with less” to ensure the viability and proper risk management of the business. Economic volatility plus rapidly expanding complexity have joined with known information security threats to create a perfect storm for executives. In the current operating environment, management teams must “own the truth” about what happens in the business if they are to traverse these unprecedented changes. Owning the truth requires controlling data assets within the company and across its trading and customer networks. If leadership teams can’t control and audit how data is used, they can’t manage risk effectively. The decision separating winners from losers will be how companies employ information security policies and solutions that protect their data assets while enabling the business in the most cost-effective manner.



Feeling lucky?

C-Suites are in uncharted territory for 2009, and probably into 2010. Continued uncertainty in the global financial system has made every company vulnerable to sudden, radical fluctuations in public sentiment, whether deserved or not.

Operating a company in such a flux will test the most seasoned leadership teams. However, a common thread links companies that successfully navigate today's treacherous waters. Regardless of the industry, the winners in the current environment "own the truth" about what happens in their business. The truth* is a single set of rock-solid facts that reflect the reality of a company's performance.

The building blocks for creating a single version of truth are the company's data assets—its customer lists, HR records, R&D specs, regulatory files, strategy documents, communications logs, etc. Controlling these data assets alone doesn't guarantee that management possesses the truth about an organization's compliance with regulation, its stewardship of customer information or its reliability as a business partner. However, it's equally clear that NOT controlling these data assets virtually assures that management is ignorant about what really happens within the four walls of the company and beyond.

In today's highly charged marketplace, ignorance can kill a company before it has a chance to respond. Regulators won't care why the right data is not available to prove compliance. They only care that it's not. Customers

won't care how their information was compromised, lost or stolen, only that it was. Traders won't care whether a rumor is true or false, only that there's money to be made exploiting it. For management facing a volatile 2009, the calculus is clear and stark. If you don't control your data assets, you don't own the truth. If you don't own the truth, you're not realistically managing risks.

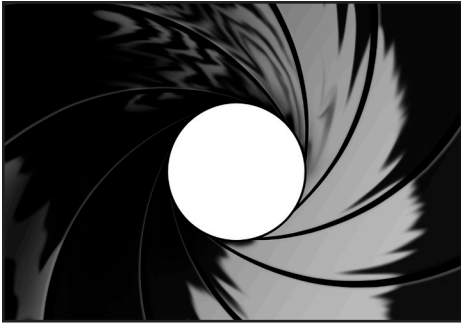
However, controlling data assets isn't simply about locking them up with security technology although there may be isolated justifications for the most sensitive data. Instead, controlling data assets is about making people accountable for their actions that involve corporate data. Building in the business processes and technical ability to audit precisely where the company's data resides, who is using it, and what they are doing with it creates such accountability.

This is where smart security techniques and technologies associated with Data Loss Prevention (DLP) come in. Now more than ever, information security must enable a business to assign accountability for its data as clear and auditable as it does for any other corporate asset like a building, an office desk or an employee automobile. Smart security based on DLP em-

powers a company to know as much as possible about all the data it's responsible for within the constraints of the business. DLP enables companies to allocate or remove rights associated with that data in real time, and do so in the most cost-effective manner. If they're implemented effectively, DLP technologies and techniques help transform the auditing function beyond "taillights"—reporting what happened—more to "headlights" which can potentially head off security breaches before they happen.

Better "headlights" are sorely needed by executives during the next few years. The known risk profile for the next 18-24 months includes an increasingly professionalized global hacker economy, higher likelihood for insider-sourced threats due to financial turmoil, as well as greater scope for human error to cascade into massive security breaches. These known risks are growing in the context of rapidly evolving complexity caused by economic pressures forcing companies to cooperate over more organizational and political boundaries in order to boost productivity in tough times.

** From the viewpoint of information security, truth is the accurate and timely intersection of data acquisition, data intelligence, and contextual understanding of circumstances that have governed the environment within which the data and its usage had transpired.*



The Year of Living Dangerously

Throughout 2009, job 1 for the C-Suite will be to survive the current upheaval in financial markets and the global economy in general. The existential threats in the macro-economy relate to and multiply the effects of well-known internal and external security threats affecting individual companies.

Massive uncertainty requires maintaining the integrity of data assets and business processes more pressing than ever. The nature of external, internal and environmental threats haven't changed. The global black market for identity information now includes organized mafias and even a few shadowy governments. Economic turmoil has turned out millions of workers with inside knowledge of security policies and even security technology. So many parts are in motion to where honest mistakes by good employees can expose a company to catastrophic risks given the current fragility.

Simultaneously, companies face these risks in an environment of tight budgets, lack of qualified information security staff, and little scope for impacting productivity in order to learn a new security system.

External threats

First and foremost, leadership teams need to face the fact circa 2009 that many, if not most, hackers are professionals rather than hobbyists. They're professionals because they create their own opportunities rather than respond to a chance opening. Speaking in the New York Times, BT's chief of security Bruce Schneier noted that most current worms and malware are now professionally written. "The criminals have gone upmarket, and they're organized and international because there is real money to be made."

In December 2008, IDG News Service reported that black market criminals were offering to sell information on over 20 million German bank accounts for 12 million Euros. Journalists from Wirtschafts Woche (Economic Week) who posed as potential buyers of the stolen data managed to obtain a CD with 1.2 million accounts after meeting the criminals in a Hamburg hotel. The CD provided names, addresses, phone, account numbers, bank routing numbers, and in some cases, the victim's account balance. It's likely that the data was collected from bank call center employees according to the magazine.

Almost hand-in-hand with the increasingly brazen activities of professional criminals has been a growing capability for open-source digital vandalism. The 2008 conflict between Russia and the Republic of Georgia over South Ossetia provided a taste of the future when security attacks can be farmed out to large groups of people. In that case, The Economist reported that several pro-Russian websites offered their readers software and instructions to perform a "distributed denial of service" (DDoS) attack against various Georgian cyber-targets. The Russian websites provided a list of Georgian government sites as well as the British and American embassies. Users launched the attack by entering an IP address and clicking a button that said "Start Flood".

The upshot for companies is that the world has become a lot more risky even as economic conditions are squeezing the ability of companies to protect themselves. Professional criminals are increasingly sophisticated because there's more booty to be had. The dangerously passionate are obtaining cheap tools to execute attacks that were previously out-of-reach.

Then there are the insiders....

Internal Risks

It's a fact that many professionals are losing their jobs in the current economic climate. It's also a fact that some of these professionals have insider knowledge of systems and procedures that raise the risk of information breaches. 2008 produced a bumper crop of insider-sourced information security lapses that put millions of customer records into play.

- August 2008: Countrywide Financial Corporation (2 million names). The FBI arrested a former Countrywide employee and an outside partner in a scheme to sell personal information, including Social Security numbers of about 20,000 customer profiles each week over a two year period. The insider was a senior financial analyst at Countrywide's subprime lending division. Files were emailed as Excel spreadsheets to buyers, often from Kinko's copying and business center stores.

- April 2008: New York Presbyterian Hospital (50,000 names). An admissions employee was alleged of selling 2,000 patient records in an identity theft scam. The employee accessed almost 50,000 names in total. Records contained names, phone numbers, and Social Security numbers of patients.
- April 2008: Lending Tree (unknown number of names). Several former employees of Lending Tree, a huge online mortgage broker, were accused of sharing confidential passwords with a handful of non-approved lenders, who used the profile information to pitch their own products to Lending Tree customers.

Almost as serious as security breaches by corrupt insiders are the honest mistakes made by employees that expose the company to regulatory or market risk. Forrester Research estimates that almost 80% of the information security breaches suffered by companies result from human error rather than malfeasance. For example, in December 2008 more than 250,000 Social Security numbers were posted online by mistake by the Florida Agency for

Workforce Innovation. The incident occurred when Excel and text files with millions of state and private employment records accidentally made it online in the course of developing a new website for the agency.

It was reported in November 2008 in Ohio that the names and SSNs of almost 1,000 employees of Sinclair Community College had been left open to public view on the Internet for a year. An Excel spreadsheet containing data on people who worked at the school during 2000 and 2001 was placed in a folder by an employee who didn't realize that the folder could be viewed online. This comes on top of eleven computer disks containing personal information on Ohio retirees and employees are missing somewhere in the postal system by Medical Mutual of Ohio during October 2008. It seems insufficient postage was placed on the envelopes containing the disks. To date, it is assumed that the disks are safe within the postal system but neither postal authorities nor management can be 100% sure of precisely where the disks reside.



Psst!!!...wanna buy a famous landmark cheap?

During December 2008, the New York Daily News took all of 90 minutes to steal the \$2 billion Empire State Building. The newspaper filed bogus paperwork with the City of New York to transfer the deed to the historic property from Empire State Land Associates LLC (the true owner) to Nelots Properties LLC. Nelots is "stolen" spelled in reverse.

The property transfer documents contained clues that should have alerted city employees to the hoax. Fay Wray of "King Kong" fame was listed as a witness. The notary signature came from the legendary bank robber Willie Sutton. According to the newspaper, the stunt illustrated a yawning loophole in the operating policies of the Office of the City Register, the municipal authority for recording deeds, mortgages and other real estate transactions in New York City.

According to the newspaper, the current system doesn't require city clerks to verify property transfer information to be true, only that the forms are properly filled out. Thus, one of the most significant tools for hundreds of millions of dollars of mortgage fraud in New York is the humble notary stamp, available at the local stationary store for about \$30.

For its part, the Daily News returned the Empire State Building to its rightful owners one day later.



Data, data everywhere

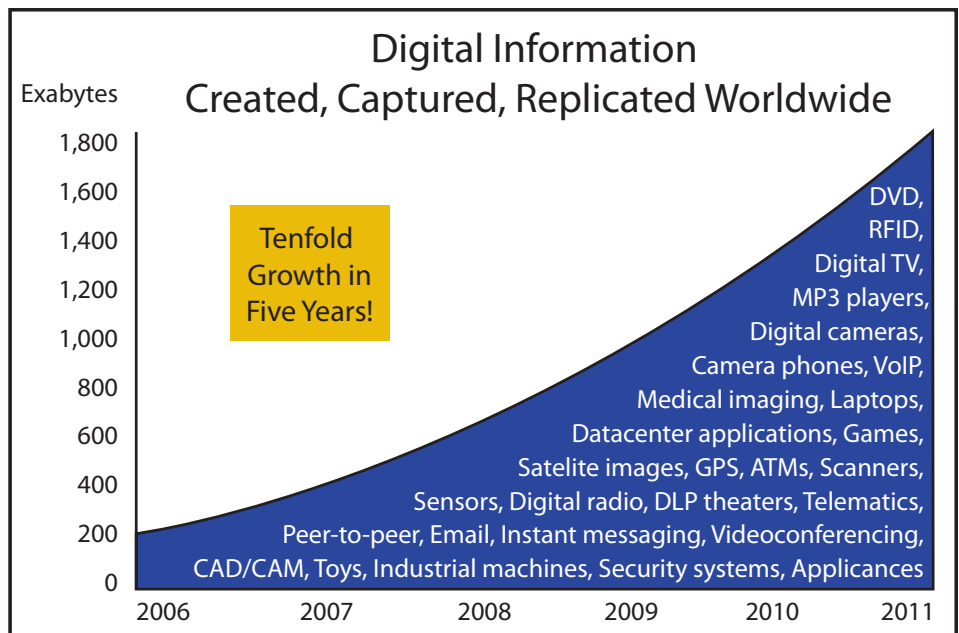
Corporate data is exploding and current information security models are struggling to keep up. It's not so much that information security technology per se is defective or that techniques for securing corporate information don't exist. Recent years have seen a dramatic improvement in information security compared to the first decade of widespread use of the public Internet for conducting business.

However, whatever gains made by security technology or technique have been far eclipsed by the rise in general complexity. The Internet has enabled networked companies to expand across the board. Therein lays the problem. Networked companies, by definition, are those who share and add value to data and communications traffic. And yet, by sharing information with other companies, individual contractors, a raft of partners and suppliers, not to mention customers, networked companies open themselves to higher risks of failure by the weakest link in the chain.

This is happening as a proliferation of client devices with massive storage capabilities makes securing networks and client devices all the more difficult. Mobile devices such as smartphones and PDAs often sport multi-megabit storage capacity. According to Cisco Systems, an 80 MB mobile device can hold thousands of MS Word documents and hundreds of thousands of emails. New portable storage devices the size of a pack of gum can hold 64 GB of data, enough to copy an entire computer hard drive yet fit in the shirt pocket of a rogue employee.

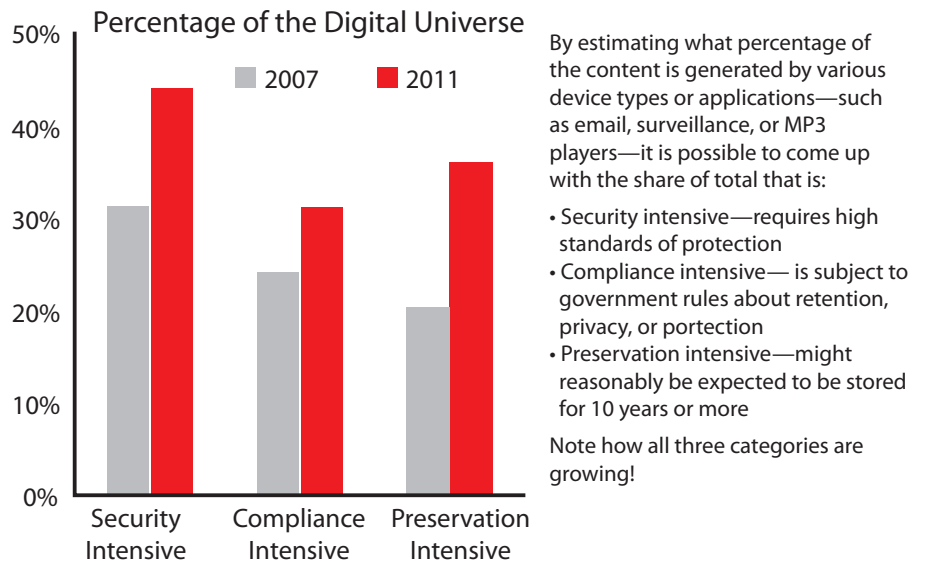
How much data is out there? Who is responsible for its security? Where do the Company's management "walls" end? Who pays? These are questions many leadership teams would love to know but often don't. Market research IDC attempted a stab at the scale of electronic data floating in the world's networks or living in hard drives. The researcher stated in March 2008 that the size of the global digital universe in 2007 approached 281 exabytes (or 281 billion gigabytes). It forecasted that the total amount of digital information would increase 10-fold between 2006 and 2011.

More sobering than the sheer scale of the data management problem is the degree that companies are responsible from a regulatory or competitive viewpoint for much of that data. According to IDC, while 70% or more of the world's electronic data is created, captured or copies by individuals, organizations have either responsibility or liability for that data at some point in time. Responsibility might be security, privacy protection, fraud detection, archiving, searching, screening for viruses or obscenity among others. This isn't academic debate. Consumers post copyrighted videos to YouTube and Viacom sues Google for a billion dollars. Just wait until portable health records triangulate between patients, doctors and insurance companies.



² The Diverse and Exploding Digital Universe, IDC March 2008
<http://www.emc.com/collateral/analyst-reports/diverse-exploding-digital-universe.pdf>

The Enterprise Faces the Digital Universe



³The Diverse and Exploding Digital Universe, IDC March 2008
<http://www.emc.com/collateral/analyst-reports/diverse-exploding-digital-universe.pdf>

Co-mingled consumer and corporate data is only fact of life for 21st century companies. Another fact of life is that companies will share this potentially hot potato with other companies as part of daily business. Networked economies, greater outsourcing and a drive for productivity have expanded service supply chains (e.g. customer support via 3rd party call centers) to exceed most manufacturing supply chains in breadth and complexity. Consistent security policies spanning multiple companies would appear to be a prerequisite for such an organizational model. But are they?

PricewaterhouseCoopers (PwC) surveyed over 7,000 senior executives world-wide during Q1 2008 to ask them about their information security policies, both internal and across their partner networks. According to the survey, fewer than half of all respondents (43%) say their organization has established security baselines for external partners, suppliers, and vendors. A little more than a third (37%) requires third parties to comply with

internal privacy policies. And less than 25% have an inventory of the third parties handling the personal data of customers and suppliers or even conduct due diligence on these third parties on their data privacy policies.

The PwC study did confirm that executives were cognizant of the inherent security risks of passing data back and forth between companies. But that awareness didn't seem to translate into stronger measures to protect data. The research surfaced major anxiety among executives regarding the ultimate reliability of their business partners as it pertains to data security. Asked how confident they were in the security practices of their partners and suppliers, a huge majority (78%) said they were only "somewhat confident" in their counterparties. The survey revealed that 10% weren't confident at all their partners' data security while 15% didn't even know.

Executives might dream of a time when the data universe wasn't expanding so rapidly or that responsibility could be cleanly demarcated.

But the genie is out of the bottle. Too much data is in motion among consumers and companies for neat organizational boxes to make much sense anymore.

What does that mean for information security? Trying to create airtight access control to the raft of digital client devices in today's companies or hermetically seal public networks is a costly game of "whack-a-mole" that current economics simply won't support. This doesn't suggest that companies give up on securing access to networks and PCs. It also doesn't mean that companies should dispense with security awareness training and education for their workforces.

What it does point to is the fact that perimeter security and training alone aren't likely to match the twin cocktails of exploding data and ever expanding complexity in a cost-effective manner.

How context-oriented DLP solutions control the data flood

The value proposition of context-oriented DLP solutions like those from InDorse Technologies is to enable company management to know its data, their respective trajectories, and control it cost-effectively. This involves setting up the processes and tools that discover and inventory into manageable groups all the data out there for which you're responsible and constantly trace its movement so you know where it's stored, how it's being used, and who is using it – and for the data that are deemed too sensitive, to enforce protection inside and outside the organization's IT administrative domain.

More specifically, InDorse helps decision makers know what data they have, classify it into manageable bundles to monitor, and effectively control/enforce policies based upon the risk profile of a given record. This enables administrators to follow the lifecycle of files or documents within and outside the company to understand who authored, touched, or changed them. Based on sensitivity of a data type for compliance or cooperation within a service delivery network, these administrators can assign rights that stay encoded within the record, regardless of where it is.

This process forces documents themselves --- rather than individuals --- to adhere to compliance mandates. For example, it might be a rule (probably a smart one!) that it is impossible to attach a customer record to an Instant Messenger session. A corollary rule might be that the record will allow itself to be attached only to email that circulates internal to the company.

Many, if not most, DLP solutions offer the ability to inventory data records with various business rules. The main question, then, is the degree that a given solution imposes costs on productivity within a company. In this case, InDorse doesn't require users to learn new security procedures or install new systems on their desktop. The data simply behaves as management intends it to behave, without asking users to change their entrenched behavior.

There is an important caveat to remember, of course. DLP solutions such as InDorse can only inventory, tag and enforce business rules connected with data. They cannot assign value to risks. Only management can do that, but InDorse provides machine-assistance to company management with detailed document lifecycle history from everywhere and content from which to make real-time decisions.

Preparedness over Prediction

The real gold of a company is its combination of data assets, the file servers and data-bases that hold the information. That's what any security solution is protecting, whether it operates at the level of the perimeter, the client device or the data record itself. The data is also what the bad guys are after, what corrupt insiders try to sell, and what innocent employees inadvertently expose.

The economic calculation for executive teams to make is how they balance the cost of prevention with the cost of a security breach involving corporate data. A 100% bulletproof security solution will stop any and everything— including the ability of a company

to make money. Economizing on information security measures saves on the front-end but assumes that the company can pick up the pieces when the inevitable happens. Hence, too much security is too expensive just as too little security is too expensive.

Determining how much to spend on security in the end depends on the extent that management teams must own the truth about what's happening in the business. The need to own the truth is a matter of course for highly regulated financial or healthcare-related businesses. Joke-of-the-day website publishers face a different risk profile. This doesn't elevate the former or trivialize the

latter. Each operating entity must manage, and in some cases mitigate, the highly concentrated risks facing everyone during 2009 and beyond. Winners in this game will approach their security decisions not from the point-of-view of whether a security solution is "secure", but whether it allows the business to be the most profitable in light of all the risks it faces.

Regardless of the internal dynamics that eventually determine how much a company perceives its risks, the currency of many, if not most, of these risks is denominated in digital data that is in constant motion. Decision-makers forget that fact at their peril.



© 2008 InDorse Technologies. All rights reserved. International Patents-Pending. This data sheet is for informational purposes only. InDorse Technologies MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, IN THIS SUMMARY. Other products or services mentioned may be trademarks or servicemarks of other companies.

770 BROADWAY • 2ND FLOOR • NEW YORK, NY 10003 • TEL +1.646.495.6127 • FAX +1.646.495.6126 • WWW.INDORSE-TECHNOLOGIES.COM