

WHITE PAPER

KILLING THE SHADOW SYSTEMS

AUGUST 2009

@ncanvas

www.encanvas.com

FACTORS DRIVING CHANGES IN OFFICE DATA MANAGEMENT

1. Securing Business Critical Information

Many companies have started to experience the consequences of non-existent, insufficient or poorly implemented data security plans. The absence of 'proper IT' to serve the diversity of information management, analysis and human-centric workflow requirements that exist in the office has created a paucity of unsecured business-critical information held in spreadsheets and micro-databases beyond the governance of IT teams. For most organizations, up to 60% of business critical information is found in these unsecured office environments.

Table1. Headline news items of data security breaches

Aug 2006:	Nationwide Building society loses laptop containing confidential data on 11 million customers
Sep 2007:	Accenture sued by State of Connecticut for losing a tape holding information on several hundred state agency bank accounts and 754 agency purchasing cards
Nov 2007:	25m people's child benefit details, held on two discs
Dec 2007:	7,685 Northern Ireland drivers' details lost
Dec 2007:	3 million learner drivers' details lost in US
Jan 2008:	600,000 people's details lost on Navy officer's stolen laptop
Mar 2008:	HSBC banking group admits to losing a computer disc with the details of 370,000 customers
June 2008:	Six laptops holding 20,000 patients' details stolen from hospital
July 2008:	MoD reveals 658 laptops stolen in four years
Aug 2008:	PA Consulting loses memory stick of Home Office data containing details of thousands of criminals

As the table above illustrates, there have been several headline cases of data security breaches over recent years - most resulting from the existence of shadow systems. Organizations have invested millions of dollars to make sure that networks and core data systems are secure. But when security breaches occur, so often the weakest link turns out to be an email from an employee, a stolen or misplaced memory stick, a laptop or spreadsheet.

'Shadow Systems' consist of small scale databases or spreadsheets developed and used by end users outside the direct control of an organization's IT department. Typically these systems are developed on an as needed basis by knowledge workers to respond to new situations that demand new information. Rather than being authored as a formal IT project, these systems are not tested, documented or secured with the same rigour as formally engineered software solutions. In consequence, shadow systems have become the biggest single source of data security breaches.

2. Shadow Systems Influence on Information Worker Productivity

Use of Shadow Systems has a huge impact on the productivity of information workers whose ability to perform tasks is limited by inappropriate tools. The experiences of office workers mirror the findings of Accenture into access to information for middle managers.

Table 2. Findings of Accenture (NYSE: ACN) online survey (January 2007), of more than 1,000 middle managers of large companies in the USA/UK to learn how they gather, use and analyze information.

Managers spend up to two hours a day searching for information, and more than 50% of the information they obtain has no value to them.

Only half of all managers believe their companies do a good job in governing information distribution or have established adequate processes to determine what data each part of an organization needs.

59% said that as a consequence of poor information distribution, they miss information that might be valuable to their jobs almost every day because it exists somewhere else in the company and they just can not find it.

42% of respondents said they accidentally use the wrong information at least once a week, and 53% said that less than half of the information they receive is valuable.

45% of respondents said gathering information about what other parts of their company are doing is a big challenge, whereas only 31% said that competitor information is hard to get.

57% of respondents said that having to go to numerous sources to compile information is a difficult aspect of managing information for their jobs.

In order to get information about competitors, customers, project responsibility or another department, respondents said they have to go to three different information sources, on average and 36% said there is so much information available that it takes a long time to actually find the right piece of data.

Part of the difficulty lies in the way managers are gathering and storing information. For example, the majority of managers in the survey said they store their most valuable information on their computer or individual e-mail accounts, with only 16 percent using a collaborative workplace such as a company's intranet portal.

In most organizations where knowledge workers operate, it is almost impossible for knowledge workers to use 'proper IT' systems to access information as they need it. Therefore, it has become accepted practice for knowledge workers to *serve themselves* by creating 'Shadow Systems' that employ accessible tools – that knowledge workers can use - such as email, spreadsheets etc. to manage the capture, management and sharing of information.

Use of Shadow Systems creates the following productivity issues:

- Information is hard to find and share
- Corporate knowledge assets remain hidden to the organization
- Human-centric information flows are not formalized and operate in a sub-optimal way with workers unknowingly duplicating effort on activities of no benefit to the organisation.
- Middle managers are unable to validate how productive their workers really are.

3. Responding to Changing Organizational Behaviors and Operating Structures

The way individual knowledge workers see themselves and discharge their roles is changing rapidly. People today work more in teams and are more mobile than they ever were. A shortage of knowledge experts is encouraging the formation of loosely coupled value networks and knowledge markets in most industries. The new choice for knowledge workers is to become self-employed or join more virtual boutique enterprises to balance their work-home lifestyles more appropriately. A new classification of business person – the 'Alter-Preneur' has emerged. These are people that start a business simply to achieve a more desirable way of life and it is the fastest growing employment group in Europe.

Organizations too are changing the way they work; seeing the need to collaborate more closely with partners and share their information with customers, partners and stakeholders to form collaborative knowledge markets.

These changes in culture, behavior and organizational structure are impacting on demands for more useful, better organised information in the office (and virtual office) where knowledge workers operate. They demand better tools for collaboration and better ways to share information; to work together when working online but geographically dispersed.

Strategies to Overcome the Threat of Shadow Systems

In response to these drivers, IT Managers are coming to identify the following business needs. To:

1. Implement effective data breach avoidance strategies to prevent business sensitive data from leaving the premises

With the increasing number of lawsuits focused on data breach and security incidents, it is crucial that all businesses take steps to develop comprehensive security policies and also to ensure that their assets will be protected in the event that those policies fail.

It is simply not an option for IT Managers to do nothing to improve the robustness of data security in the office environment. Neither is it a complete solution to assume that employees will encrypt every file that they hold on a memory stick or laptop hard drive.

Recent case examples point to the following 'high threat' areas of data security being compromised as the result of Shadow Systems existing in the office:

- Knowledge workers encounter a new business situation that demands a new repository of data is formed but due to lack of accessible or affordable 'robust IT' systems, they turn to self-help solutions they can build themselves with accessible tools.
- Knowledge workers are unable to interrogate data from back-office systems in the way they need to and this results in the data be transferred to spreadsheets and unsecured environments in order to facilitate its analysis or manipulation.
- Knowledge workers are unable to transfer data securely with partner organisations resulting in data being exported from secure data environments to unsecured data formats.
- Knowledge workers need to work with information beyond the office walls so they transfer data from secure data environments to their mobile computing device.
- IT software developers are unable to develop new software applications without first exporting data into a development environment.
- IT software developers are unable to install the software they need to develop new business applications on the locked down laptop they are using so they export data to an unsecured laptop that allows them to use the development tools they need.

All of the above can result in documents and Shadow Systems being saved to laptop drives and USB memory sticks in unsecured formats.

2. Know what data is being held where

Few IT heads can say they know what data is held in the office environment. Up to 60% of business critical corporate information is thought to reside within informal office networks. Much of this information is in people's heads, in documents or PC and laptop hard drives. Increasingly, data is also held on mobile computing devices and memory cards.

3. Prevent the formation of 'Shadow Systems' that results in:

(a) Data from being held in places where it can not be found by others

When data is dispersed in knowledge worker authored documents and information systems, it very often falls beyond the visibility of search and data management tools that can interrogate its content to harness the corporate intelligence that exists within it. In the 1990's Intranet software burst on the scene to manage this type of information. However, self-governance of document taxonomies and databases in many cases led to greater disorganisation of data rather than less.

(b) Knowledge workers from in-advertently losing business critical information

It is not uncommon for data to be lost under the following circumstances:

- A file is lost due to a hard-disk or file corruption and data has not been backed up.
- A file holding critical data is inadvertently misplaced or saved over and cannot be recovered.

To prevent data loss, proper IT protocols of good data governance need to be applied to information tasks in the office that use business-critical and sensitive information such as customer, competitor, industry and financial data.

(c) Knowledge workers from maliciously or in-advertently using wrong or out of date information

When knowledge workers are not operating robust IT information systems they are likely to encounter (and create for themselves) versioning and data accuracy/quality problems such as:

- Several knowledge workers work on the same content at the same time resulting in no coherent single version existing.
- Knowledge workers pick out a file which has been superseded.

According to US industry research, 80% of CFO's point to enhancing security and integrity of corporate data as a critical component of Sarbanes Oxley compliance registering that simple things like spreadsheet errors are a huge threat. In one case a spreadsheet error at a major financial institution was deemed a significant factor in a \$1B financial statement error in the classification of securities. An unapproved change to a formula in the spreadsheet caused the misstatement. In another example a utilities company

took a \$24M charge to earnings after a spreadsheet error - a cut and paste error - resulted in an erroneous bid for the purchase of hedging contracts at a higher price than it wanted to pay.

In circumstances where fraud is intended, spreadsheets yet again represent a major threat to organizations that encourage the operation of Shadow Systems and spreadsheets. In one reported case a trader at a bank was able to perpetrate fraud through manipulation of spreadsheet models used by the bank's risk control staff. The spreadsheet was obtained from the trader's personal computer which included figures for transactions that were not real. This fraud continued for months.

Organizations continue to employ thousands of spreadsheets for:

- Operational tasks - such as listing of open claims, unpaid invoices, inventory tracking, project management, sales pipeline tracking etc.
- Analytical/Management Information - management decision making tools, reports on corporate goals/objectives, market and trend analysis etc.
- Financial - financial statements, transaction reporting etc.

A report by auditors PriceWaterhouseCoopers in 2007 into spreadsheet use in large organizations (in support of Sarbanes Oxley 404) found that 90% of spreadsheets contain data accuracy errors whilst spreadsheets with more than 200 lines have almost 100% probability of error.

4. Help employees differentiate between secure and personal data

According to an IDC Survey in 2005, 1 in 10 workers has stolen a database or business contact details from the office and 29% of people surveyed said it was acceptable to take sales leads from the workplace. But very often, organizations fail to communicate to knowledge workers what information they use falls under the category of business sensitive and what systems and devices they are able to use in order to exploit data without exposing it to security threats.

5. Honour compliance standards

IT managers are bound by law to store, backup, encrypt, secure and protect their confidential data, and demonstrate that they are doing this satisfactorily. In addition to standards such as International Standards Organization's ISO 17799, known as ISO 27001 in Europe, each organization will face its own blend of country and industry specific compliance requirements.

- US Sarbanes-Oxley Act of 2002 affects any company listed on the US stock exchange and requires strict internal controls and independent auditing of financial information to defend proactively against fraud. Resulting Sarbanes-Oxley audits will direct attention towards data security issues and create a wake of actions that IT managers must seek to comply with.

- In the UK, organisations must adhere to the Data Protection Act 1998 if they hold information on members of the public.
- In Financial Services the Payment Card Industry introduced the PCI Data Security Standard, to ensure member organisations secure their online transactions and data.

It is common for solutions to target 'proper IT' when responding to these demands which secures known IT systems and the networks that knowledge workers use. Case studies show however, that data breaches more commonly occur within Shadow Systems environments which do not fall within this area of scrutiny because they are not recognized to exist.

Evaluation of Options

So what can IT Managers DO about the problem of data security in the office resulting from the existence of Shadow Systems?

In terms of procurement options Encanvas believes there are three possible solutions:

1. To adopt strict access protocols to business-critical data

It is not always possible to totally prohibit access to core business data to knowledge workers without the participation of the IT team; particularly when IT resources are so scarce. Even when this can be achieved, it remains likely that knowledge workers will continue to develop spreadsheets and databases themselves that result in new data – that is business sensitive – from emerging.

2. To secure the use of spreadsheets by adopting file security software

There are a number of software tools available today to control how users access the Shadow Systems they create. Files that are downloaded or shared are automatically logged and encrypted by a file security management server. Whilst this overcomes some of the more obvious security threats it does not prevent the proliferation of Shadow Systems and the security and data management issues they create.

3. To procure specialist software

Another alternative is to procure specialist software designed specifically to provide an affordable and realistic alternative to Shadow Systems that IT and business users' value. It is this approach that is the focus of this document.

Resolution of Concerns

When considering specialist software to overcome the security threat of Shadow Systems, what does the software need to do?

Encanvas believes what is needed is a means of rapidly formalizing the creation of robust IT systems that exploit the advantages and use of relational databases in response to knowledge worker needs for situational application. This rapid 'across-the-desk' authoring capability supported by easy-to-use and familiar data analysis and manipulation tools is needed to displace the use of, or need for, Shadow Systems.

The systems purchased to displace Shadow Systems must support the features one would expect of a robust IT solution (and that do not exist in spreadsheets!) including:

1. Documented operation
2. Change control process
3. Access control process
4. Version control process
5. Security
6. Integrity of data

In addition to the above, business necessity means that knowledge workers must be able to respond to *new business situations* by creating and working with *useful* information as they need to – given that users are so accustomed to the versatility of desktop tools such as spreadsheets and word processors. Solutions should support 6 key functions in support of knowledge worker requirements; giving them the capability to:

1. Acquire and transform existing data from back-office (core) systems (supporting different formats) and from third party sources to form new composite applications.
2. Assimilate new data by direct data entry, from colleagues or third party sources using online data entry forms and geo-spatial data capture tools delivered through a secure portal environment.
3. Analyze and 'work' with data in a user defined environment with the ability to execute formulas and visualizations, reports, execute formula and data transformations, compare data sets etc.
4. Use data remotely using mobile computing devices whilst operating in a data secure environment and ensuring that data transfers are also secure.
5. Form secure portals to enable individuals to collaborate within a secure workspace adopting robust (RDMBS) data management.
6. Create a global index of documents and unstructured content across the enterprise to enable the organization to realize its corporate data assets and manage its data risks.

2. IT Performance & Compliance Considerations

Solutions should meet standard selection criteria for any enterprise application including:

- User Administration – Must support a customisable security model that includes Single Sign On (SSO)
- Network Security – Data must not be able to be removed from the data management environment without
- Web Security – Must support SSL and not permit downloading of unsecured data assets. Pages should not require downloaded components. Pages should be served on demand to prevent hacking. Web server and applications server should run on separate processors.
- Data Security – Data should be held in a robust RDBMS system (ie. SQL Server or Oracle). Data requests should adhere to RDBMS protocols.
- Code Security – Software should be authored in a standard code development environment, fully documented and covered by ESCRO agreement.
- Operating Systems Support - Must adhere to de facto industry standards
- Scalability and Performance Tuning - Must scale and follow documented procedures for performance tuning

3. Supplier Credentials

Software vendors should demonstrate the following credentials:

- Track record of supplying software into business-critical applications
- Demonstrable security and scalability of solutions
- Case examples that demonstrate business value

Encanvas Unique Features and Implementation Considerations

Encanvas software protects data in the office by formalizing information management and human-centric workflows in a way that makes knowledge workers more productive.

What Makes Encanvas Different?

Encanvas:

- Creates a Secure Office Data Environment that places data management for knowledge worker applications under the governance of IT without introducing inflexibility in the tools that knowledge workers use.
- Incorporates highly advanced data acquisition and integration layer that enables data to be acquired from different sources and files formats without coding. It also includes a component to formalise non-human interventions such as data uploads.
- Produces secure portal and mobile applications by publishing ASP.NET and .NET Framework systems whilst ensuring data is held securely within a relational Database Management System at all times.
- Responds to demands placed on IT teams for situational applications by adopting a no-code 'point and click' single integrated development environment that supports the lifecycle of applications authoring. It means that applications can be authored across-the-desk with knowledge workers to ensure they receive robust IT solutions that meet their information needs right-first-time; thereby removing the need to self-author Shadow Systems.
- Provides an out-of-the-box suite of powerful data mining, manipulation, visualization, reporting and analysis tools – all of which can be authored without coding or requiring additional tools.
- Offers rich collaboration and business intelligence tools so that knowledge workers can improve the way they work together.

Implementation

Encanvas can be deployed as a network appliance to simplify implementation and because no programming skills are required, training takes only a day. Within a week IT teams can be authoring enterprise scalable composite applications.

Through experience gained in a series of successful deployments, Encanvas has developed a robust 10-stage agile project development methodology.

About Encanvas

Encanvas[®] software makes the workplace work better.

We bring added value to the Microsoft[®] enterprise platform by creating the technologies organizations need to spend less and receive more from their software investments.

We've created the world's first Integrated Software Platform; digital equivalent of the micro-chip. Our Secure&Live[™] platform enables the design, deployment and operation of applications without coding or scripting all made possible by a single tightly coupled architecture. It facilitates the massive scaling of portal architectures; so users can communicate, share information and their applications in real-time while operating in 'secure spaces' that protect systems, data, identity and intellectual property.

Similar to the influence of the micro-chip in electronics, our integrated software platform is creating a mushroom of innovation around the world as individuals and organizations realize they now have the tools to design and publish right-first-time software applications to cloud computing platforms at very low cost and risk – serving the long-tail of business applications needs.

Encanvas also creates Social Operating Systems (see Encanvas Squork[™]). In the digital era a network is a group of people tied by relationships, not a set of computer systems strung together by wires. User-centric computing enables web workers to 'work efficiently anywhere' while organizations can achieve a step-change in productivity by harnessing the enthusiasm, skills and collective intelligence of social networks.

Intellectual property

All information of whatever kind and which is contained in any documentation, drawings, specifications, diagrams, plans, notes, data, patterns, models, samples, software, software applications, computer outputs or other materials or records or other information whether written or oral of a business, financial or technical nature which is marked or otherwise indicated or known to be of a confidential or proprietary nature shall be called for the purposes of this project 'Confidential Information' and remains the property of Encanvas Inc.

Encanvas Inc.'s appointed data controller is Mr Nick Lawrie. Further information is available on request.

Contact information

Encanvas Inc.

One Exchange Place
Suite #900
Jersey City NJ 07302
(Americas) +1 201 524 9600
(Europe) +44 1208 700525
www.encanvas.com

All trademarks and trade names used in this document are acknowledged as belonging to their respective owners. Whilst every effort has been made to independently validate and interpret the completeness and business value of vendor offerings, insights have been captured from published materials and may therefore not accurately reflect the opinions and views of suppliers.

Encanvas is a registered trademark of Encanvas Inc. All other trademarks and trade names contained in this document are recognized as belonging to their respective owners.