

vigilancepro

Data Loss In A Downturn – 10 Steps to Protecting High Value Information, Assets and IP



AN OVERTIS SYSTEMS WHITE PAPER

© Overtis Group Limited

JANUARY 2009

CONTENTS

1	INTRODUCTION	3
2	DATA LOSS IN CONTEXT	4
3	10 PRACTICAL STEPS TO PREVENTING DATA LOSS	5
3.1	STEP ONE: USER EDUCATION & AWARENESS AND THE NEED TO KNOW	5
3.2	STEP TWO: AVOID PATCHING POINT PROBLEMS WITH POINT PRODUCTS	5
3.3	STEP THREE: IDENTIFY CRITICAL INFORMATION ASSETS & INFORMATION FLOWS	6
3.4	STEP FOUR: APPLICATION USE - INTELLIGENTLY MANAGE CUT AND PASTE	7
3.5	STEP FIVE: SYSTEM ADMINISTRATORS AND PRIVILEGED USERS	7
3.6	STEP SIX: IMPLEMENT A FORMAL EMPLOYEE ENROLMENT AND DEPARTURE PROCESS.....	7
3.7	STEP SEVEN: ACCEPT THAT USERS ARE INGENIOUS.....	8
3.8	STEP EIGHT: USE ENCRYPTION	8
3.9	STEP NINE: DON'T RELY ON PASSWORDS ALONE.....	9
3.10	STEP TEN: STOP DATA WALKING OUT OF THE FRONT DOOR	9
4	OTHER BENEFITS OF ADDRESSING THE INSIDER THREAT	10
5	SUMMARY & CONCLUSION	10
	ABOUT OVERTIS GROUP LIMITED	11

1 INTRODUCTION

In the last 12 months 'data loss' has become the topic of intense mainstream media coverage in the UK. Whilst research consistently shows the problem is growing, it is by no means a new phenomenon.

According to USA Today (in an article published in December 2007) 162 million records were reported lost or stolen in 2007, triple the 49.7 million that went missing in 2006.

Part of the increase is almost certainly attributable to the increasing amount of legislation that forces organisations to disclose data breaches – which started with California Senate Bill (SB) 1386 that came into effect on July 1 2003. Today most US states and an increasing number of other countries have similar legislative requirements. With forced disclosure comes increased accountability and other positives. First, individuals are notified that their details have been lost or stolen. Second, the true extent of the problem is more accurately understood. And third, organisations do more to protect personal data in the first place.

For the last 10 years all major security studies have highlighted clearly that insiders represent the biggest threat facing organisations. The most recent UK BERR Information Security Breaches Survey 2008 reported that only 13% of organisations identified unauthorised outsiders on their networks.

Mainstream media attention - whilst raising awareness to the issue of data loss - has also meant that the term 'security' now has more widespread negative connotations. This doesn't help security professionals or enlightened business leaders who see security as an enabler, rather than a disabler. In fact, when security is applied sensibly and appropriately as part of a formal structured risk management process, it has entirely positive value.

It is a matter of painful fact that we are in a deep downturn. Margins are being squeezed and budgets are being cut as economic conditions worsen. There is a clear correlation between data loss (and the wider insider threat) and the state of the economy. A recent report by KPMG highlighted that losses in the three months from August to November 2008 were already higher than the first eight months of the year. It also predicts that data loss incidents will increase dramatically in 2009 to more than double the level in 2008.

The reason for this is two-fold. The insider threat is undoubtedly heightened when people are losing their jobs and employees are generally uncertain about their futures. Companies often use more contractors and outsource functions during difficult times in an effort to control or reduce costs – the corresponding insider threat rises as the workforce becomes more transient and is one step removed from corporate controls.

Individuals who have lost their jobs are taking more than memories away from the office: an enormous amount of valuable data is walking out on iPhones, iPods, USB flash drives, laptops, DVDs and CDs. Human nature can be extraordinarily generous, but also incredibly mean-spirited.

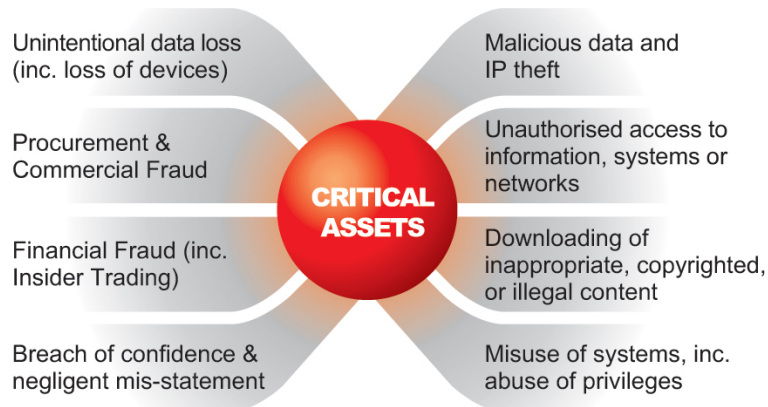
Ex-employees may steal data to give them a competitive advantage in their role with a new company, or simply to cause operational or reputational problems for the organisation he or she has just left. It doesn't matter which of the two provide the catalyst – the result of either is a major impact on the company.

The second reason the insider threat increases in a downturn is that the international highly-organised criminal community see it as a clear opportunity. Individuals, concerned about their personal finances, can be more easily persuaded to deal in information. Criminals pay surprisingly good money for detailed consumer databases containing full personal details, particularly if the data includes date of birth and the 3 or 4 digit credit card security code (CVV / CVC / CVV2 number).

This white paper focuses on simple steps – combining policy and process, with technical controls - that will ensure that data is not lost in a downturn, profits are protected, and competitive edge is not eroded.

2 DATA LOSS IN CONTEXT

Unintentional data losses, as well as malicious data theft, are just two examples of insider threats. Insiders are responsible for the majority of data losses as well as commercial, procurement and financial fraud. Other insider threats include negligent mis-statement, breach of confidence and inadvertent formation of contracts (particularly via email).



With the increased adoption of outsourced services and third party network connections the definition of the insider has evolved. Historically insiders were simply full or part-time employees. Today the term 'insider' refers to anyone with in-depth knowledge of internal systems, organisational structure, processes and procedures, or with trusted access to systems, networks and the information they contain.

It is critically important to understand that the majority of insider perpetrated breaches are not down to the malicious insider but due to accidental or unintentional actions. The 2005 CSI/FBI Computer Crime Survey reported 52% of incidents were due to employee mistakes and carelessness. More recent research from The Computing Technology Industry Association on IT Security and the Workforce, amongst others, suggest that 77-80% of incidents are down to quite innocent entirely unintentional user error.

Solutions put in place to address data loss – and the wider insider threat – should be designed to promote positive user behaviour in line with stated policy with softer 'learn as you work' user mentoring features as opposed to unexplained blocking of activity. If the latter approach is taken the result is often a dramatic operational impact that culminates in Help Desk meltdown.

3 10 PRACTICAL STEPS TO PREVENTING DATA LOSS

3.1 Step One: User Education & Awareness and the Need To Know

Raising staff awareness of security through a structured education and training programme will pay dividends; literally. It is the single most important soft initiative that will make the single most important impact to overall security posture. At a minimum consider republishing security policies internally and running training courses for all users.

The code-breaking activities of Bletchley Park remained a true secret until well after the conclusion of the Second World War because of rigorous security education and training of staff, coupled with the need to know (N2K) principle. Bletchley Park is probably the greatest historical example of 'where there is a security will, there is an operational way'.

The need to know principle states that information is exclusively restricted to people that have a need to know it. However, there is an alternative perspective. A company should grow its knowledge base through actively providing information in a push feed to the right people in the right format at the right time. Information is, after all, power.

Effective endpoint solutions can achieve this with no loss of business efficiency or effectiveness. In a downturn, increasing efficiency is more important than ever.

3.2 Step Two: Avoid Patching Point Problems with Point Products

The second step to take is to avoid falling into the trap of focusing on yesterday's crises. In other words, it is not particularly useful to provide point security products to counter something that has already gone wrong.

Point products are like putting an Elastoplast on a victim of blood poisoning. You might seal the original entry wound, but the poison is already spreading. A more systemic approach to treatment is necessary. This will involve the integration of information security solutions with physical systems to achieve a far more comprehensive systemic defence mechanism.

The recent volume of stories of major data losses and IT-enabled crime and fraud (or unchecked user misuse of systems over time) are more than sufficient evidence that traditional security point products – largely designed to protect other products – are not addressing the threat. The focus needs to move to how users interact with (process, store and transmit) sensitive information.

In order to address insider threat comprehensively a fundamentally new strategy and approach is required. The number of possible 'data leakage vectors' available to users in a typical enterprise environment, combined with the levels of ingenuity that come with a strong (often financially motivated) intent to remove data, means quite simply that point solutions are not practical or effective.

Point solutions are unlikely to adapt to new data leakage vectors as they arise – they've consistently failed to historically. Five or six years ago the threat posed by instant messaging and social networking applications was entirely unforeseen. When these applications arrived existing security solutions did little to address the risk of information dissemination associated with their use.

Controls need to be placed where they are effective - between the user and the information. Not on the network or at the gateway.

3.3 Step Three: Identify Critical Information Assets & Information Flows

The third step is to take a dive into the deep end of the information pool, and establish what information is where. Information, once identified, can be properly audited and protected.

For even a medium size company this step can – at first - appear as daunting as the 11,674 steps that make up the entire Mount Niesen staircase. Take it one flight at a time.

Identify the obvious and most critical assets. Critical assets will be those containing sensitive or regulated financial, personnel and customer data, or that constitute part of the intellectual property of the organisation within the information estate.

Depending on the nature of the business these may include:

- sensitive employee and customer databases
- source code
- designs and drawings
- product roadmaps
- marketing strategies and pre-release material
- critical strategic and competitive analyses
- financial spreadsheets and results
- sales information and forecasts
- board minutes
- executive communications
- internal announcements
- mergers and acquisitions plans and files relating to other confidential projects.

There is a good chance that policy already states that sensitive information should be saved on particular network drives and shares – such as a finance drive accessible only by people in the Finance team, HR data accessible only by HR, or product information accessible only by R&D or Engineering staff.

If Microsoft Active Directory is used then leverage the investment already made to come up with a matrix of assets and the users / groups that should have access to them. Then add to the matrix a list of file level actions that should be allowed (and disallowed) based on approved information flows. Think at the 'whole file' level – should Finance be able to copy spreadsheets from the finance share to local hard drives or to removable media? Who should be able to print files, attach them to emails, rename or delete them?

Information discovery or ediscovery solutions may be helpful providing they aren't used in an attempt to automate this step completely. Identifying that there is potentially confidential information, everywhere, is of limited value. Manual identification of assets combined with technical controls that monitor content in real-time is often a far more powerful approach – and for one thing has the major advantage that information identified is 'currently confidential', in that users are actually accessing it 'now'.

Where third parties, including outsourcing partners, are given access to critical systems strongly consider the use of terminal services to provide a secure gateway into the network. Terminal services can be used to efficiently segregate key information assets into secure containers with granular control over user access and the actions they can perform once authenticated.

Even internally the use of terminal services, transparent to the user, can deliver sophisticated security solutions across multiple user profiles.

Using terminal services for enhanced security is covered in depth in a separate Overtis white paper.

3.4 Step Four: Application Use - Intelligently Manage Cut and Paste

The next step in preventing data loss is to consider user interaction with information below the whole file level. Advanced insider threat management solutions can not only explicitly allow or disallow the use of particular applications (through the use of white and black lists) but also functions available to users within particular applications.

When a highly sensitive file is open it may be appropriate to monitor or even prevent user actions such as cut, copy, export, save as, and PrtSc. Print (particularly to PDF) is often an additional concern. Furthermore restrictions may depend upon not only content but also context – such as time, or location. Some users may require access to key files remotely out of hours. Others may not.

3.5 Step Five: System Administrators and Privileged Users

In an Insider Threat Study conducted by CERT and the US Secret Service that analysed 23 incidents in the banking and finance sector in detail, technical staff were implicated in 72% of them (38% system administrators, 20% programmers, and 14% were IT specialists).

In a more recent survey published by Computerworld in August last year, 88% of the 300 IT administrators interviewed admitted they would take corporate secrets, if they were suddenly made redundant. The target information included CEO passwords, customer databases, research and development plans, financial reports, M&A plans and the company's list of privileged passwords.

When selecting technical controls the ability to monitor and manage the actions of system administrators and privileged users should be high up on the selection list. Equally secure log servers should be considered to ensure that a tamper-proof audit trail of system, security and event logs are available, along with change management and file integrity solutions on critical servers.

3.6 Step Six: Implement a Formal Employee Enrolment and Departure Process

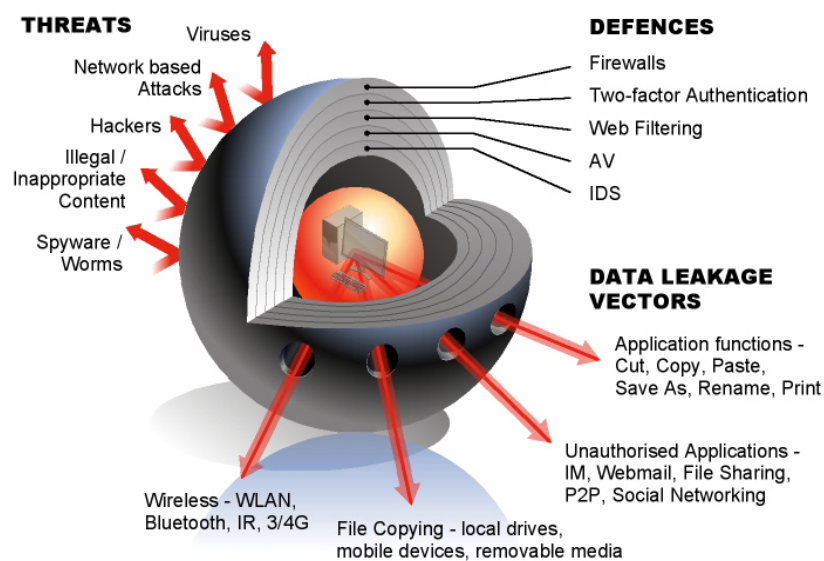
A haphazard informal process for dealing with employees joining and leaving the organisation represents an unacceptable risk in the current climate. A joining procedure should be in place to ensure that new starters only have access to the resources and information appropriate to their role and responsibilities.

When someone leaves the company there should be a formal process for handling their departure – ensuring that access to email and other systems is revoked quickly. Any company provided hardware – including notebook PCs, Blackberries and other mobile devices – should be taken from the individual as soon as their employment is terminated.

3.7 Step Seven: Accept that Users are Ingenious

Data Leakage Vectors available to determined insiders are numerous. And not all are obvious (such as multi-function devices that will copy a document placed on the glass straight to a PDF, in memory, and email it out to any email address entered on the LCD screen).

Within any user population there will be a small number of individuals that will push the edges of acceptable use guidelines, bend the rules, and find ingenious unforeseen ways around whatever controls are put in place. Just as a very small percentage of the sheep population in Wales worked out after cattle grids were first introduced that they could lie down, roll over, and restore their freedom to roam the valleys (suicidal kangaroos will be covered in a forthcoming white paper). It is important to remember that 98% of the user population will be reasonable upstanding trustworthy people.



Many companies considering data loss prevention lose sight of the original and primary purpose of the project - often quite early on - and get irrationally fixated on theoretical ways in which users could or might remove data through the most obscure means. Avoid lengthy debates about risks that represent 0.05% of the spectrum.

Focusing on the major data leakage vectors and channels will improve an organisation's security posture and risk profile dramatically. Keep it simple initially - according to the BERR ISBS 2008 survey 67% of companies do nothing to prevent confidential data leaving on USB sticks and 84% do not scan outgoing email for confidential data.

3.8 Step Eight: Use Encryption

Given the headlines over the last 12 months needless to say it is a very good idea to encrypt sensitive data on mobile devices and removable media. Transparently to the user, whenever possible.

3.9 Step Nine: Don't Rely on Passwords Alone

The ninth step is to recognise that the world has changed. Positive proof of identity is required to ensure proper authentication of actions, transactions and operations. The use of biometric devices can mitigate against session hijacking and suspicious or malicious activity on an endpoint. Finger vein readers are faster, more accurate and less open to subversion than fingerprint devices. Lifting a fingerprint and creating a latex copy is relatively easy.

A significant number of South Koreans are known to have entered Japan in the last 6 months using 'special tape' to alter their fingerprints. Altering the pattern of your finger veins is more invasive and comes with the added comfort to the user that the finger itself must be attached to something with a pulse.

As numerous organisations have discovered in the last 12 months, to their cost (literally, reputationally and in terms of sheer embarrassment), a low-cost device would have prevented a high-cost incident. High security does not have to mean high prices. However, low security does normally mean high impact.

3.10 Step Ten: Stop Data Walking out of the Front Door

The tenth step is the integration of physical security measures with information security solutions. The aim is to stop data walking out of the door and disappearing into the thin air of cyberspace without an audit trail.

Solutions are emerging that integrate logical (IT) security solutions with physical and electronic systems (such as CCTV, physical access control systems and RFID). Extending physical security and combining physical with logical (IT) security controls can provide powerful policy management and enforcement of:

- Visitor and contractor access - and attempted access.
- Entry or attempted entry to computer rooms and data centers.
- Access to secure cages or racks within facilities.
- Visual monitoring of hosting environments.

A full visual audit trail of date and time stamped events is provided with attached supporting evidence from door entry and/or camera systems - which may prove invaluable in the event of hardware tampering or theft. Integration with access control systems enables:

- Enforcement of 'low man count' policies with the option to prevent access to sensitive data, or to certain applications or application functions, if occupancy of a given area drops below pre-determined levels.
- The ability to freeze user sessions if the user leaves a given area to prevent unauthorised access through session hijacking.
- Ability to freeze all workstations in a secure area if the area is empty (overnight, during breaks, or as the result of a fire alarm)

Integrating physical and logical security systems maximises existing investment, improves risk management and realises tangible security, operational and financial benefits through increased efficiency and synergy.

Integration is being driven by increasing cross-functional cross-business unit risk discussions and a move away from a disconnected focus on individual elements of the security lifecycle. Enterprise security roles are changing. Individuals that previously held isolated positions with a narrow logical (IT) or physical security focus are moving to broader based multi-disciplinary roles, working more closely together to manage and minimise risk across the business as a whole.

4 OTHER BENEFITS OF ADDRESSING THE INSIDER THREAT

In addressing the insider threat organisations often derive significant additional benefits.

First a comprehensive audit trail is often provided of events across all user activity providing a unique insight into how users interact with sensitive information. Regular review of event types and volumes can be used as the basis for tuning of rules to prevent certain actions, or to strengthen and improve controls.

Insider threat initiatives therefore support on-going compliance and continuous review of controls for applicability and effectiveness based on actual user activity and behaviour. The rich audit trail provides answers to difficult questions from internal and external auditors and demonstrates action taken to identify, measure, mitigate and manage risk.

Audit trails containing actual desktop screenshots, screen captures of web browser and other application windows, and even CCTV images, enable powerful visualisation of exactly what users are up to. WTUSIWYG – What The User Sees Is What You Get.

Secondly the information gathered as part of insider threat programs can be used to analyse user activity – highlighting areas where productivity and efficiency can be improved. In a climate where ‘do more with less’ is increasingly the mandate from the boardroom this data can prove invaluable.

5 SUMMARY & CONCLUSION

Businesses are surfing ahead of a wave of data loss. Those that don’t use the right balance of policy, process, technology, user education and training – combined with regular improvement reviews - will get wet.

Every major company that has suffered a significant well-publicised security breach has seen the value of its shares fall - and not recover to the pre-incident price for 18 months.

At a time when businesses are under significant pressure to do more with less, and cutting costs by reducing headcount, the insider threat is increased – individuals losing their jobs pose a significant risk and employees that remain are destabilised, uncertain about their future and financial security. No organisation needs the additional negative impact of becoming the subject of tomorrow’s headlines.

Careful selection of insider threat management solutions – within a strategic ITM program involving user education and awareness activities - can realise significant benefits.

Not only is the risk of data loss reduced but companies also obtain a unique insight into user activity. With minimal analysis of the information gathered about how users interact with information, areas where efficiency and productivity are sub-optimal can be highlighted. With this knowledge companies have the opportunity to shape user behaviour. Increased productivity and efficiency at a time when the economy is slowing down can only be a good thing.

ABOUT OVERTIS GROUP LIMITED

The Overtis Group Limited - founded in 2003 - is an integrated security solutions business specialising in the protection of high value physical, human & information assets on a global basis.

Overtis Group utilises the proven resources and experience of its divisions Overtis Systems and Overtis Solutions to discretely architect, deliver and support integrated security solutions to high risk government departments, public sector bodies and the enterprise community.

Overtis Group has developed its expertise, capabilities and product & service offerings to allow organisations to realise the benefits of truly comprehensive strategic security planning, underpinned by the rational integration of physical and logical (IT) security systems.

Within the group's DNA is in depth security experience provided by personnel who've quietly succeeded in the international arenas of high-value government, military and commercial security & information management and assurance.