# KEEPING UNSTRUCTURED DATA SECURE

## IN AN UNSTRUCTURED WORLD

Watchful®

Keep IT secret.

The most recent study by the Ponemon Institute shows that 90% of CIOs and their staffs interviewed admitted that they have had a leak/loss of sensitive or confidential data in the prior year. And, half expect it to happen again

## EXECUTIVE SUMMARY

Hardening the network perimeter to keep attackers out does not suffice anymore. One needs to also secure the data itself whenever and wherever. Despite efforts to strengthen defenses, control unsecured devices, restrict the usage of social networks, and otherwise mitigate the risk of cyberattack, users remain the weakest link in information security

Organizations of all sizes are challenged to protect a growing quantity of valuable digital information against careless mishandling and malicious use. The increasing incidences of information theft underscore the need for better protection of digital information.

If recent history (WikiLeaks, Yahoo, LinkedIn, information leakage of personal client data, etc.) teaches us anything it is that confidential information is not secure in its traditional form and access to information is not controlled at all.

This digital information may include confidential e-mail messages, strategic planning documents, financial forecasts, contracts, dynamic, database-driven reports, and other sensitive information. The growing use of computers and devices to create and work with this information, the introduction of extensive connectivity through networks and the Internet, and the appearance of increasingly powerful computing devices have made protecting enterprise data an essential security consideration.

In addition to the threats of theft and mishandling, a growing list of legislative requirements adds to the ongoing task of protecting digital files and information. For example, the financial, government, healthcare, and legal sectors are increasingly taxed by the need to better protect digital files and information due to emerging legislative standards.

How does a Chief Information Officer, then, control what happens to this data, especially if the greatest threat isn't the 'bad guys' breaking into the network, but the 'good guys' letting the information out in ways and to places they shouldn't?

According to recent studies by IDC, information leakage is mainly accidental (>50%) and in the majority of known cases implies a direct cost higher than 100,000 US$. Follow up studies show that the five year cost of a confidential data breach is, on average, over $6M USD

## WE HAVE MET THE ENEMY... AND THEY ARE US!

Today's information security professional is paranoid, and for good reason – corporate information is the most valuable asset that most organizations have, outside of their people. The breadth of damage that can be caused if that information is breached, lost, leaked, stolen, etc. is almost incalculable.

According to the Net Diligence 2013 Cyber Liability and Data Breach Insurance Claims study, the average data breach cost $3.7M. And there is a developing market; the Global Knowledge Expert Reference Series quotes in a recent whitepaper, "There is a growing underground black market for the sale and distribution of product information and company secrets."

Yet it's not always a foreign government or offshore hacker group that is the issue – according to Global Knowledge's report of the Top 10 CyberThreats for 2013, #7 is Insider Violations. These can be accidental (sending a sensitive email and erroneously having autofill put in the wrong email address, thereby leaking to an unintended source), or malicious (such as the well-publicized case of the auto company executive who sold future product plans to a foreign competitor).

This data has led today's information security professional to realize that you can secure the perimeter of the network all you want...the most significant threat is the 'trusted insiders' that come and go across that network boundary daily. Not only can they make mistakes, but the prevalence of USB devices, smartphones, internet sharing sites, etc. means that the ways that information can get out are legion. Does this mean that it's a fool's errand to attempt to secure information against insider breach?

Actually, no. The process and technologies exist to take simple yet powerful steps to protect your information, without handicapping either the employee's ability to work or the company's ability to be agile with regards to its information flow. By following a simple four-part plan for information security, you can go a long way to ensuring that your organization doesn't become another financial loss statistic.

"IDC believes the majority of information leaks will continue to be accidental..." – IDC, 2010

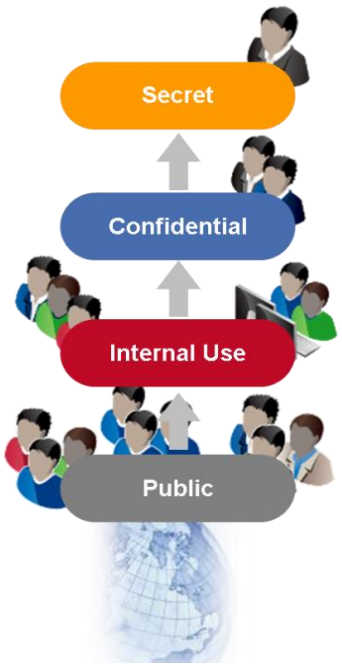
## STEP ONE: DEFINE YOUR INFORMATION SECURITY MODEL

Most well-run companies have policies that documents (printed) that are sensitive in nature must contain a footnote, or watermark, or other identifier with a disclaimer that they are confidential and/or sensitive in nature. Advanced companies have a richer model, normally with levels such as Internal Use Only, Confidential, and Secret, for example.

These levels correspond to the level of sensitivity of the information contained therein, and serve two purposes: a) to remind the employee that this is valuable information that shouldn't be released to anyone unauthorized, and b) to mitigate the company's liability if this does get out, showing that there was at least an attempt at a document control policy to restrict unauthorized access.

However, with the digital age of information, we haven't kept up with implementing and managing this information security model...even though massively confidential information is easily sent anywhere, anytime through email, in documents and spreadsheets, or placed in internet file sharing sites such as DropBox or Google Drive.

Today's CIO and/or CSO looking to protect their company's information are leading their companies to define levels of classification for sensitive information, such as:




1. **Public**: information that can freely be shared with anyone

2. **Internal Use Only**: business policies and procedures that should remain within the organization, hence only employees should have access

3. **Confidential**: information which, if leaked, could cause loss or harm to the company (such as costing, pricing, customer lists, etc.); possibly only management may have access here

4. **Secret**: information which, if leaked, could cause significant financial or reputation loss to the company (strategic plans, M&A investigation, financials, trade secrets, margins, HR information ,etc.) and hence only senior management should have access

Once this model is established, information can be assigned into these levels as it is created. This begins the process of controlling where this information can and can not go, and who can and can not use it, not only as it's created but throughout its lifecycle.

The 2011 "Cost of Data Breach" study done by the Ponemon Institute showed that 33% of breaches were caused by insiders and that the minimum cost of a data breach was $566k, with the average cost being $4.5M.

A 2013 Verizon study supports this, showing that 69% of security incidents are caused by insiders

## STEP TWO: CLASSIFY YOUR INFORMATION

Once you have your model established, information should be classified into it as it is created. This can be done one of two ways – manually, by the author, or dynamically, according to policies established by the company.

Most users in an organization are good citizens, and want to assist in protecting the company if they can…and if it doesn't take them too far from their normal workflow.

Advanced data-centric security solutions allow information to be classified as it is saved (in the case of documents, spreadsheets, presentations, etc.) or as it is sent ( in the case of messages and emails).

This means that if a user is consciously thinking about what type of information this is that they are creating, they can easily classify it using their normal tools (Word, Excel, Powerpoint, PDF, etc.) when they hit the 'save' button.

However, there are times when the company won't want to rely on voluntary (and remembered) compliance. Some things, by their nature, should automatically be classified based upon either their content (the information contained in the email, document, etc.) or their context (who is creating it, where it is stored/sent, formats, etc.). For example, the company may have a policy that all confidential information.

## STEP THREE: PROTECT YOUR INFORMATION

Quite simply, the best way to protect your information is to have it encrypted. There are many different types of encryption, and people employ encryption at different parts of the equation (on the drive, in transit on the network, etc.).

Experts today, however, are agreeing that instead of encrypting where the information is (the drive, the network, etc.) if you simply encrypt the information itself then it's protected regardless of where it is. If it's on a laptop drive, it's encrypted. If it's in transit across the network, it's encrypted. If it's in a file sharing site such as DropBox, it's encrypted. If it's on a USB key hanging around someone's neck, it's encrypted. What that means is that this information is persistently secure… regardless of whether it in inside or outside of your network boundaries.

"Senior management understanding of the risks related to confidential information is surely going mainstream." – Aberdeen Group, 2013

## STEP FOUR: ASSIGN YOUR USERS APPROPRIATE CLEARANCE LEVELS

If a company follows a simple information security model as outlined above, it's a fairly simple matter to then assign employees to the level of information that is appropriate to them. The ubiquitous use of Microsoft's Active Directory for identity management and authentication makes this a fairly straightforward task.

For example, all employees in the AD domain can be globally assigned Internal Use clearance. This means that they have unfettered access to emails, documents, financials, etc. that are classified as Internal Use; in some companies, all emails that are being sent only to employees are automatically classified as Internal Use, for example, in order to ensure sound prophylactic measures are taken.

Management team members throughout the organization can be assigned Confidential clearance, as a part of their roles. The company has obviously already seen fit to bestow a higher level of trust and responsibility in these employees.

Senior management, a much smaller and more manageable group, could be assigned Top Secret clearance. By virtue of their position in the organization, they are normally working with this type of information and should be able to have seamless access to it when needed.

With more advanced data-centric information security solutions, you can introduce departmental scope to the levels of clearance. For example, you may give someone in the Finance Department that is a lower level employee access to Confidential information, but only that which is specifically classified as Finance in nature.

Likewise, an engineer may be granted Confidential or even Secret clearance, but only for information which is classified as R&D. Through this multi-dimensional model, you can create a simple matrix to assign users to with regards to their information security clearance levels.

Once users are assigned their appropriate clearances, the 'heavy lifting' should be done and the system should manage it. As users create and send information it can be automatically classified based upon its content and/or context, and if it falls into the wrong hands, it is encrypted and that unauthorized user will not be able to access or read the information, and will simply receive a message that he/she does not have the appropriate clearance for it

"Often residing outside of traditional databases and data structures, a typical business or government organization stores many thousands of files containing sensitive non-financial data in shared folders on file servers and NAS devices" – 2012 Business Case for Business Protection, IBM and The Ponemon Institute

## MAKE YOUR USERS PART OF THE SOLUTION, NOT PART OF THE PROBLEM

The task of keeping sensitive corporate information safe shouldn't fall solely to the Chief Information Security Officer…in a company of 10,000 employees, there is no way that one executive, even with a team of dozens of professionals, can ride herd on the entire employee base.

Instead of stopping at the acknowledgement that insiders are the greatest potential threat, turn that around and make them the greatest allies in securing the information. While this may sound like an unrealistic dream, it's actually quite simple.

1. **First**, employ information security tools that are seamless and don't force the user to go to a third party product or set of menus to use it. If, instead, your tools are integrated into their standard workflow, the user resistance is slashed and they quite comfortably assume their role.

2. **Second**, ensure that your information security solution not only protects your information, but subtly assists you in evangelizing the message. Classified information should be automatically but visibly identified as such, so that the employees know that they are dealing with important, classified data. They often take pride in this, and it drives their awareness that this is something that they are entrusted with by the organization.

3. **Third**, hold regular (bi-monthly, for example) brief information security trainings via webinar for your employees only. Give them awareness of the data breaches that are occurring in the industry, and what it costs companies when this happens. Those losses have to be made up somewhere, and your employees don't want it to be at their expense.

Even give them tips and techniques as to how to keep their personal information secure in the world of online banking and shopping, social networking, etc.

This shows that you care about them as individuals, that you are adding value as their employer, and the benefit is that an employee who is security conscious at home will definitely bring that into the workplace.

"Segmenting or classifying your organization's confidential information and intellectual property is a cornerstone for protecting it." – Aberdeen Group, 2013

## SUMMARY

History has shown that it's simply not enough to 'secure the network perimeter', as our greatest risks are that a trusted insider will create an accidental or even malicious breach.

This means that while we do want to have a secure network perimeter, we need to be more conscious about securing the information, itself.

Companies should define an information security policy which allows information to be classified into different levels of sensitivity, protected using strong encryption, and ensuring that only users with appropriate levels of clearance can access and decrypt that information.

If the company takes this approach, along with a well-intentioned effort to ensure that all employees know how to keep their personal and corporate information secure, the massive losses associated with data breaches can be largely avoided, meaning greater profits, a healthier business, and happier executives.