Dynamic Data Classification with RightsWATCH

Most organizations have spent time, money, and thought putting into place an Information Control Policy (ICP) that outlines what types of information are important to the organization, how this information should be handled, and who should have access to it. Unfortunately for most organizations…the process ends there, with the policy definition. In today's world, this can be the basis for disaster. RightsWATCH is centered on allowing organizations to control and protect their sensitive and confidential information, and to protect against information leakage, by dynamically applying the defined IPC to all types of unstructured information (emails, documents, spreadsheets, presentations, etc.) as that information is created.

Is your information safe?

Sensitive and confidential information has become the lifeblood of the organization, providing direction, competitive advantage, and protection. This is why information protection has become a top initiative for most organizations. And protecting that information starts with properly classifying information as it is created, so that it can be handled appropriately at all levels of the organization.

Security Executives that…	
Experienced breach in last 12 months	98%
Consider BYOD a major risk	71%
Consider unstructured data greater risk than a database	70%

RightsWATCH exemplifies what today's information security experts know about protecting confidential information: rather than investing all of your time and effort in trying to keep people from getting to where data is stored, it is wiser to ensure that that data can't be used even if they do get into your network. By addressing the issue right at the point of origin, the organization has much higher confidence that risk is mitigated and the proper treatment of that information can be applied by users throughout its lifecycle.

Implementing an Information Control Policy

Most organizations have thought through their ICP to outline key precepts such as

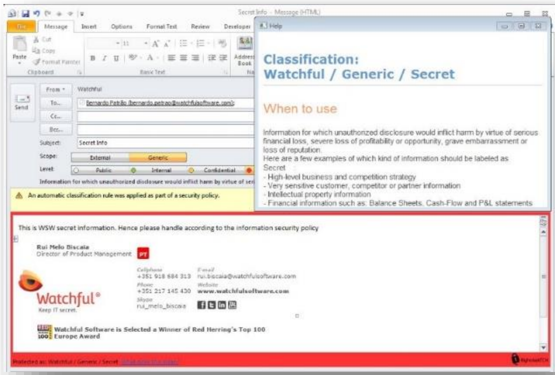
1. What levels should we have; i.e. Internal Use Only, Confidential, Restricted, Secret, etc.?
2. What characteristics should information at each level have, such as watermarks, footnotes, legal disclaimers?
3. Who should be able to have access, to what level of information? For example, all users get Internal Use, management only get Confidential, top management gets Secret, etc…

While the CISO and his/her team may have done a thorough job determining the answers to the questions above, and even defining a policy in accord with that, the cold reality is that the implementation and enforcement is normally done at the weakest link in the chain – by the users. This is not to say that the users are negligent, simply that they are not security experts. Even in well-run organizations, the average user doesn't know the ICP details, what should be categorized at what level, how to apply watermarks and disclaimers, etc. Further, to ask them to do so would be a severe distraction to their primary jobs. So, then, how does an organization ensure that its policies are implemented and enforced?

RightsWATCH's Dynamic Classification Policy Engine

RightsWATCH leverages the powerful Multi-Level Security Model (MLS) concept, in which organizations can define levels of information classification (for example, Public, Internal, and Confidential) as fits their policy. Once configured with the organization's model, information is classified as it is created, right at the point of origin. Emails are classified as they are sent, documents and spreadsheets as they are saved, etc.

This is accomplished by RightsWATCH's policy engine, which can analyze both metadata, content and context of information as it's created to apply these policies. For example, if an email contains a certain text string such as "pending merger", or data that is in a particular format such as a Social Security Number designator, that email can automatically be classified and marked without the user deviating at all from their workflow.



From: Watchful
To...: Bernardo Petrão (bernardo.petrao@watchfulsoftware.com);
Cc...
Bcc...
Subject: Secret Info
Scope: External | Generic
Level: ○ Public ● Internal ● Confidential ●
Information for which unauthorized disclosure would inflict harm by virtue of ser

⚠ An automatic classification rule was applied as part of a security policy.

**Classification:
Watchful / Generic / Secret**

When to use

Information for which unauthorized disclosure would inflict harm by virtue of serious financial loss, severe loss of profitability or opportunity, grave embarrassment or loss of reputation.
Here are a few examples of which kind of information should be labeled as Secret
- High-level business and competition strategy
- Very sensitive customer, competitor or partner information
- Intellectual property information
- Financial information such as: Balance Sheets, Cash-Flow and P&L statements

This is WSW secret information. Hence please handle according to the information security policy

Rui Melo Biscaia
Director of Product Management PT

Watchful® Keep IT secret.
Cellphone +351 918 684 313
Email rui.biscaia@watchfulsoftware.com
Phone +351 217 145 430
Website www.watchfulsoftware.com
Skype rui_melo_biscaia

Watchful Software is Selected a Winner of Red Herring's Top 100 Europe Award

Protected as: Watchful / Generic / Secret

Characteristics Matching Classification

Once information is classified, RightsWATCH can apply the characteristics specified by the ICP. For example, if the policy calls for information classified as "Internal Use Only" to have a watermark across the page in a light grey color, this can be automatically applied to documents, spreadsheets, presentations, etc. without the user involvement. Further, since this is driven by the classification metadata, the watermark cannot be removed by the users, giving the organization strong compliance and audit protection.

Not only can the information be visually marked, but classified information gets a digital 'fingerprint' at the time of creation. Through this method, the organization can begin to determine the magnitude of their classified informaiton, and see immediately how much of their information is classified, at what level, and who is originating/creating this information. For highly secure information, a further step can be invoked to have the information encrypted such that only an authorized user can open or view that file.

Confidence in your Information Control Policy

Implementing a solid ICP is the first step to protecting sensitive/confidential information. The benefits to the organization are clear and proven:

- Increased user awareness and education
- Significantly reduced liability in the event of breach or exposure
- Tighter audit controls
- Ability to influence behaviour for internal and external parties

More info at: www.watchfulsoftware.com and info@watchfulsoftware.com