Towards a Global Framework for Corporate and Enterprise Digital Policy Management [1]

Jean-Henry Morin, Michel Pawlak

University of Geneva – CUI
24 rue General Dufour, CH-1211 Geneva 4, Switzerland
{Jean-Henry.Morin, Michel.Pawlak}@cui.unige.ch

Abstract. While DRM has now matured to be a recognized and established domain it is currently struggling with interoperability issues mainly on a sector basis (entertainment and media, mobile, enterprise). In the enterprise sector, DRM was fueled by corporate scandals leading to compliance issues mandated by emerging regulatory frameworks. In this context, we make the case for the necessity of raising the debate at the policy management level (DPM) as the strategic dimension of DRM. We further argue that in doing so, enterprise information systems will have to factor in persistent protection, governed usage and managed content which represents a major challenge in this field for the coming years. A general framework is proposed in this direction to capture corporate digital policy management.

Keywords: Enterprise DRM, Digital Policy Management, Compliance, Corporate Governance

1 Introduction

Digital Rights and Policy Management has become a domain in full expansion with many stakes which are by far not only technological. They also touch legal aspects as well as business and economic as described in Becker et al (2003), Rosenblatt et al (2001). Information is a strategic resource and as such requires a responsible approach of its management almost to the extent of being patrimonial.

Let us mention as an example some recent cases such as the loss by UPS of a parcel containing the information of 3.9 million clients of a Citigroup company. Or the loss of personal data of 600'000 current and former Time

[1] This work was supported by the Swiss Secrétariat d'Etat à l'éducation et à la Recherche SER under grant No. 03.0391-1 within INTEROP Network of Excellence (IST-508011), Task Group 7 on Interoperability Challenges of Trust, Confidence/Security, Policies and NFA

Warner employees while in physical transport. These only represent a couple of recent examples of “known” cases of information theft, leakage or disclosure that most companies would have rather not disclosed. This is probably not new but what changed in recent years and “forced” disclosure of such information lies in the compliance with emerging regulatory frameworks.

Digital rights and Policy Management is now well established mainly in two distinct sectors sharing the same fundamental underlying technical principles. On the one hand the entertainment and media industry and on the other hand the enterprise sector. This paper mainly focuses on the latter.

The objective of this paper is twofold. First it is a plea for raising awareness on the strategic nature of using Digital Rights Management technologies in the corporate environment for Digital Policy Management. To this end we propose a basic guiding framework for corporate policy management. Second, assuming this awareness, we argue the corporate information systems landscape is on the verge of a profound transformation by which systems will have to factor in persistent protection, governed usage and managed content. In other words, to become “rights enabled”. A key challenge facing the DRM industry still remains to be tackled with interoperability issue both at functional and semantic levels. Proprietary incompatible solutions could represent a major legacy and problem for the future. It is thus critical to both address the interoperability issue and the strategic dimension of digital policy management. Interoperability is currently addressed within several initiatives such as for example the Coral Consortium, or the EU INTEROP Network of Excellence.

This paper is organized as follows; we briefly introduce the corporate and enterprise sector in section 2. Section 3 presents the issue of regulatory frameworks, compliance, risk and corporate governance. Section 4 discusses DRM technology in this context. In section 5 we present a general framework for corporate policy management, before conclusions and ongoing work in section 6.

2 The Corporate and Enterprise Sector

Nowadays, Enterprise Information systems orchestrate complex processes requiring fine grained business engineering skills and competencies in order to deliver, in a sound, accurate and cost-effective way, the dynamically evolving services they need. Therefore, this sector is about to witness one of its most profound and significant transformation from the point of view of information management and its organizational and information systems impact.

Currently, information protection still mainly relies on perimeter based security and access control approaches whether in the local intranet or through a VPN using secure communication channels. However, outside these boundaries it remains a critical issue rarely taken into consideration. This is all the more significant given the broad availability and use of mobile and external storage devices such as USB keys, CD, DVD, PDA, removable hard drives, etc. All things considered, from the moment information leaves the perimeter or any form of secured extension, and by any means, it is as if it were in *clear* on the Web. Consequently, the established relationships among parties are based on trust. From a Corporate point of view, this simple form of trust relationship is becoming increasingly insufficient simply considering the incurred risk and the strategic nature of information.

Policy management nowadays also suffers major gaps. It has now become common to receive emails or electronic documents having an upfront statement in bold reading the policy under which it is provided. Or a statement saying "CONFIDENTIAL, DO NOT FORWARD UNDER ANY CIRCUMSTANCES, PLEASE". Wishful thinking with close to zero effect. Forwarding risks, whether intentional or not, are non negligible. This simple example sows by itself, while we have definitely passed the point of no return of using electronic mail, at what point organizations are left without means in such situations. Corporate policies still mainly reside in dusty handbooks often provided to employees upon starting the job. In their most advanced form, these are documented on the corporate intranet basically for ease of maintenance and update reasons. In most cases, corporate policies are split among common sense and on the job experience of employees. Rare are those companies having instrumented policies by systems enforcing them, and none to this date and to the best of our knowledge, have full fledged global corporate digital policy management in place. This is a major issue and challenge we have to face in the coming years for this sector.

2.1 A few facts and figures

In order to further assess some of the key motivations of this domain, let's consider a few facts, figures and trends. According to the 2001 *FBI Crime Survey*, information theft has caused the greatest financial damage of all security related problems. A 2002 *PriceWaterhouseCoopers* report revealed that 32% of the worst security problems are caused by insiders. The *Gartner G2* revealed in 2003 that most companies loose intellectual property through employees, whether intentionally or by inadvertence. The *META Group* estimated in 2004, that by 2006 about 20% the global 2000 companies would use Digital Rights Management technologies. Etc.

These are a few quotes which are representative of a growing uneasiness in the field of enterprise and corporate security. This uneasiness materializes a fear facing a security phenomenon which is still by far embryonic: the strategic importance of Information as a resource and asset, as well as the mitigation of its associated risk.

2.2 Information : A Strategic Resource

Information has become a strategic resource for corporations. It has become critical and increasingly considered as an asset in digital form: “digital asset”. The term asset reveals its financial and *business value* dimension requiring it to be managed accordingly.

It concerns every corporate functions whether it is HR, legal, accounting and finance, sales, suppliers, customers, budget and planning, production, marketing, design, R&D, competition, analysis and simulations, tax reporting, internal control and compliance, and the list goes on and on. None of these functions whatsoever escapes this rule of requiring to be considered as a corporate asset. They all handle more or less sensitive information, be they static or dynamic, requiring various levels of protection and rules governing their use at all time and no matter where they reside.

When mentioning dynamic information, we are referring explicitly to all the dynamically generated data by application portals, ERP systems, databases, line of business applications, etc. often ending up in spreadsheets or files, thus escaping any form of control and protection allowing them to be freely transferred to removable storage devices or worse sent by email to a personal address to further work at home.

3 Regulatory Frameworks, Compliance, Risk and Corporate Governance

The economy and the corporate world have been recently under heavy pressure due to several scandals thus raising major concerns for investors and markets. It is in this context that several regulatory frameworks emerged defining principles of practices, responsibilities (now criminal) as well as the duties of publicly traded companies.

Among the most striking example was probably the *Sarbanes –Oxley Act* governing the integrity of financial and accounting data. Another example in the banking industry is the *Basel II* agreements requiring banks to comply by 2007 in order to minimize as much as possible the level of their reserves.

By now, there are many such regulatory frameworks either sector based, or by type of risk, etc. These issues now have a direct impact on corporate governance in the sense that compliance is not only mandatory and bound in time, but must also be audited on a regular basis. The cost of not complying is crippling and may even lead to sever penalties, fines and jail or even stop the business with disastrous consequences on reputation and image. DRM technologies can help up to a certain point in managing these issues and thus mitigate such risks.

Among the most widely known regulatory frameworks which were or still are on the compliance agenda, we find: (classified by activity)

- ***Financial services***
  Graham-Leach-Bliley (1999) Title V – confidentiality of customer banking data
  Sarbanes-Oxley (2002) – integrity of financial and accounting data
  NASD 2711 (2002) – relation between research analysts and investment banks
  Bale II – (2007) level of reserves based on operational risks
- ***Health***
  HIPAA (1996) – confidentiality of patient records
  FDA 21 CFR Part 11 (1997) – data integrity of drug clinical studies
- ***Other***
  California SB 1386 (2003) – confidentiality of personal data
  ISO 17799 (2000-2) – best practices for information security
  Etc.

It is noteworthy to mention that the compliance issue is a sustainable problem which is here to stay, having a recurring audit activity in order to prove and assess compliance on a permanent basis. It is therefore vital for corporations to place this issue high on the agenda not only from specific risk mitigation point of views but also and more importantly at the strategic level of corporate governance. This requires a consistent approach which is global to the enterprise, involving everyone at all levels, as well as defining the most accurate management dashboards for its continuous monitoring. Thus, Digital Policy Management becomes a strategic project under the supervision and responsibility of the top management. It will be only at this price that companies will be able to cope seamlessly with such issues in a cost effective way. Thus allowing to capture not only the evolution of the existing regulatory frameworks but also the emerging and future ones we cannot anticipate but are bound to appear on a regular basis.

4 DRM in the Corporate and Enterprise Sector

DRM technology represents the technical means to manage digital assets and define the rules governing their use in a persistently protected way. It relies on the basic following principles common to all sectors where DRM is used:

- Superdistribution (Mori (1990, 1987), Cox (1994, 1996),
- Persistent protection,
- Definition and expression of rules governing usage and access to digital assets using rights expression languages (Stefik (1996),
- Direct or indirect association of these rules to the digital asset.

4.1 What can DRM do –and not do in the Corporate Environment

DRM technology can address and help solve a number of issues becoming increasingly critical in the corporate environment. In particular, it represents a solution for the digital management of rights and policies governing content usage as well as the processes and electronic services. Most common examples are among the following:

- Enables a responsible management and use of digital assets within and outside the corporate perimeter
- Helps in managing classifications (e.g. company confidential, board of directors, projects, etc.)
- Helps instrument compliance management with respect to regulatory frameworks and corporate policies at large (e.g. Sarbanes-Oxley, HIPAA, NASD2711, etc.)
- Helps in managing retention policies (e.g. emails, documents, etc.)
- Provides the means to manage issues facing traceability, monitoring, tracking, usage metering, audit trails, etc.
- Provides a centralized management of revocation and granting (e.g. new employee, employee leave, etc.)

However, DRM technology does not and never will provide total “military grade” security. The issue is to find the right balance between security and a commercially viable risk level. Or, in other words, security stops where the marginal cost of implementing it is disproportionate to the risk one is trying to mitigate. Moreover, technology cannot provide any protection against analogue attacks like reading information over the phone, taking a picture or hand copying. Such cases are however clear and leave no doubts on the malicious intentions thus allowing to take legal or disciplinary measures.

4.2 Digital Rights Management: a Help rather than a Constraint

Let us mention here that it is not a question of adopting a paranoid attitude aiming to the total and absolute control of everything aka “big brother”. It is rather a responsible and aware attitude and clear general policy with respect to information management representing one of its most invaluable assets and intellectual property.

Given such a context, DRM technologies can provide a more pleasant and safe work environment substantially reducing numerous risks of unintentional errors. It represents a help providing potential risk detection and mitigation.

Let’s consider a particularly striking example to illustrate this. It is now common to work on several projects involving many people and partners. Moreover, it is also not uncommon to be allocated to different projects at the same time. Email remains a widely spread and used tool for communication and coordination among the project members. Now, how many times do we diligently and carefully check the recipient list when doing a “reply all”? The most frequent and honest answer is “almost never”. However, it is possible that some people leaving for a few days decide to use another more convenient personal address to keep in touch with the project. Now consider one of these persons be fired with immediate notice while away.

Well, in such a situation, if no one pays attention this person will continue to receive emails on his personal address until someone realizes it, if ever. Thus having access to information he is no longer entitled to receive he could easily disclose it to the competition or the media. Moreover, if this person still holds work related data on mobile or removable devices he will still be able to access it freely.

This is exactly one among many information risk situations, for which DRM technologies can provide significant help in applying and verifying dynamically corporate policies applicable to specific situations. Moreover, by applying consistently those policies to work documents, an employee leave would immediately triggers the revocation of his rights in a centralized way thus preventing further access to held documents provided the policy required some form of on-line license acquisition.

5 A Framework for Corporate Policy Management

We propose a general framework for studying, analyzing and defining corporate policy management towards its partial digital instrumentation. Our starting point is a basic layered architecture commonly found in the enterprise by which security issues are categorized by infrastructure,

application and content. These three layers traditionally fall under the responsibility of IT and IS involving the CTO, CIO and CSO.

We then introduce another layer for Corporate Policy Management, under the responsibility of the top management including CEO, CFO, CCO and COO. To be noted that the compliance officer (CCO) has moved from traditionally known “internal controls” to a top management position and responsibility, mainly in the light of compliance issues. This layer is strategic and focuses mainly on corporate governance. In the scope of corporate policy management, we identified three main sources of inputs in two distinct categories. The first category is internal and deals with internal corporate rules and policies. The second category is external and has two sources. The business practices commonly applicable for the activity sector and the legal and regulatory frameworks the company must comply with.

Now, across these four layers, the three technology ones and the strategic one runs a recurring audit activity to monitor and assess compliance. Traditionally undertaken by external auditors, it is also the case that such activities are fundamental from inside the enterprise for corporate governance reasons using management dashboards and indicators. Figure 1 illustrates this general framework for corporate policy management.

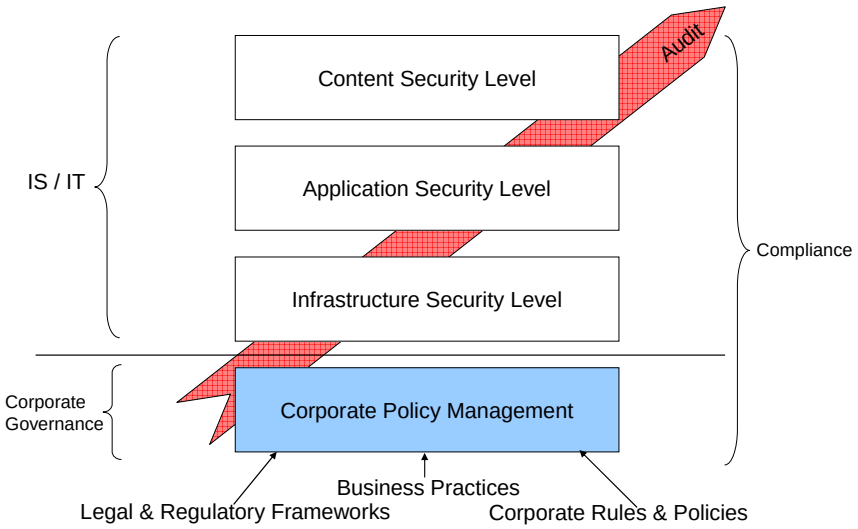

Figure 1. *General Framework for Corporate Policy Management*

Given such a framework, it provides the means to analyze those policies in order to determine the ones that can be partially or fully digitally instrumented by technologies such as DRM at IT and IS level. To be noted that definitely not all policies can map to technical solutions. A good

example of this would be the notion on “intention” when accessing a report for example within NASD 2711. Intentions will hopefully remain hard to calculate in the future. Nevertheless, part of the corporate policy management will be instrumented and the remaining will stay under the control of traditional measures. The instrumented part will provide the means to answer questions such as: who, what, when where, traces, delegations, etc. Figure 2 places corporate policy management with respect to its sources and its potential digital instrumentation using Digital Rights and Policy Management technologies.

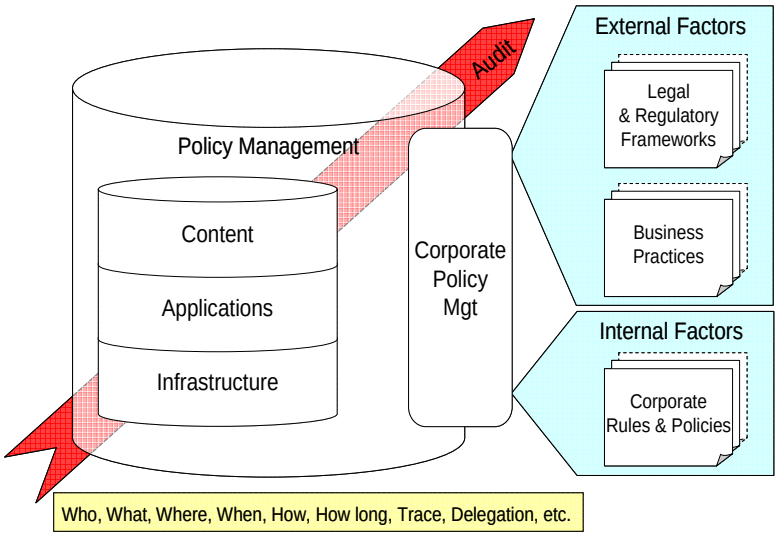

Figure 2. *Positioning of Corporate Policy Management*

6 Conclusion and Ongoing Work

Digital Rights and Policy Management represents a founding technology and a major strategic issue in the light of a responsible, sustainable, cost effective and perennial approach to modern information systems. DRM technologies encompass the instrumental dimension of the issue (i.e. the means) while Digital Policy Management (DPM) cover the strategic dimension consisting in capturing, analyzing, specifying, representing, evolving, and managing internal and external policies before instrumenting those that can be through DRM technologies.

We have proposed a general framework for studying, analyzing and defining corporate policy management towards its partial digital instrumentation. We acknowledge this is still very preliminary ongoing work requiring much further work to refine, validate and implement the necessary models and tools at the corporate policy level to capture, design, define technical requirements to be implemented by underlying technologies, monitor, evolve, assess, audit and manage corporate policies. Current leads considered for further work include investigating the recent evolution in the ISO/IEC 15504 standard towards a general process oriented framework. Other relevant frameworks (e.g. COBIT, ITIL, etc.) will also be studied from the point of view of alignment, risk management, corporate governance and business value. Links with Enterprise Architecture frameworks will be investigated and requirements engineering techniques could prove to be particularly useful in initial phases of defining and formalizing policies from unstructured heterogeneous sources. Finally, let us stress that in such a perspective rights and policy enabling the corporate information system represents a mandatory major challenge for the years ahead.

Références

Becker E., Buhse W., Günnewig D., and Rump N., (eds.), (2003) Digital Rights Management, Technological, Economic, Legal and Political Aspects, LNCS 2770, Springer Verlag, 2003.

Cox B., (1994), “Superdistribution”, Wired Magazine, September 1994, pp 89.92.

Cox B., (1996), “Superdistribution Objects as Property on the Electronic Frontier”, Addison-Wesley, 1996.

Mori R. and Kawahara M., (1990), “Superdistribution: The Concept and the Architecture”, Transaction of the IEICE, Vol. E 73, no. 7, July 1990, pp. 1133-1146.

Mori R. and Tashiro S., (1987), “The Concept of Software Service System (SSS)”, Transaction of the IEICE, J70-D.1, Jan 1987, pp. 70-81

Rosenblatt B., Trippe B. and Mooney S., (2001), Digital Rights Management: Business and Technology. New York: Hungry Minds/John Wiley & Sons, 2001.

Stefik M., (1996), “Letting Loose the Light: Igniting Commerce in electronic Publication. In M. Stefic “Internet Dreams: Archetypes, Mythes and Metaphors”, Cambridge, MA, 1996.