NOTICEBORED

Management briefing on

IPR metrics

Summary

This discussion paper proposes and discusses information security management metrics relating specifically to Intellectual Property Rights (IPR).

Introduction

Managing and ideally optimizing our IPR-related controls (namely the activities needed to reduce the chances of being prosecuted by third parties for failing to comply with their copyright, patents, trademarks *etc*. plus those necessary to protect our own IPR from abuse by others), requires us to monitor and measure them so that we can get a sense of the gap between present and required levels of control, apply corrective actions where necessary and improve our performance going forward.

IPR requirements (targets and limits)

Upholding/complying with third parties' IPR

Full compliance with third party IPR may not only be unreasonably expensive to achieve in practice, it may actually be against our best interests. We acknowledge that failing to comply fully with third party copyright, patents and trademarks *etc*. may expose us to the risk of legal action and/or bad publicity, and that it may damage relationships with third parties. On the other hand, relatively few IPR abuses are detected and/or result in prosecution, meaning that IPR compliance controls may a waste of money in many cases although, *a priori*, we cannot be certain which controls are essential and which are superfluous. Therefore we seek a **balanced** and **dynamic** approach (shown diagrammatically in Appendix A), balanced in the sense that we should apply suitable controls to uphold third party IPR where the risk of being caught in contravention is judged to be greater than the cost of compliance, and dynamic in that we should periodically review the risk appetite in line with the threat of legal action by third parties. This implies that management should proactively monitor and respond to IPR risks and controls.

Although the 'optimum control point' identified on the graph would be our ideal target position, we need to take uncertainty into account. This is a theoretical graph which would be extremely difficult to measure and plot in practice. Furthermore, the graph would surely change over time due to the 'dynamic effects' shown (*e.g*. if the software industry launches a campaign to identify and prosecute software pirates, the risks and costs of non-compliance increase at least for the duration of the campaign). Erring slightly on the side of caution and ethics, our target control point is therefore identified on the figure.

The target point may be defined by management in several ways *e.g*.:

- Setting a cap on IPR control costs (budgeting and investment management);
- Setting targets for the number of actual IPR non-compliance incidents in a year or, perhaps more usefully, the number of IPR non-compliances detected by internal audits and reviews (assuming that these represent the level of risk);
- Monitoring trends of incidents, risks and controls and adjusting the control levels dynamically by increasing or decreasing expenditure (tricky!).

Protecting our own IPR

In relation to our own IPR, the situation outlined above is reversed but the model shown in Appendix A remains basically sound. As the level of expenditure on IPR controls (such as proactively monitoring the Internet for signs of abuse of our copyright materials and trademarks) increases, we are likely to increase our returns at first through successful prosecution of offenders but, in practice, we would probably notice diminishing returns beyond which further efforts would be uneconomic. It is up to management to set the level of investment in IPR controls as they see fit, and to monitor this decision periodically (*e.g*. during the annual budget).

By analogy to the case noted in Appendix A where a third party successfully prosecutes us for IPR infringement leading to additional charges from others, so there is probably some value in being seen to take a proactive stand against abuse of our IPR. Publicity surrounding a successful case against an IPR abuser seems likely to have a deterrent effect on others. We therefore recommend setting a minimum target of at least one successful and publicized case per year.

Measuring and reporting on IPR (metrics)

Control costs

We can monitor and manage the costs of IPR controls within the existing information security management system, budgets *etc*. Here are some examples of IPR control costs:

- Internal recharges for time and effort to prepare/review policies, standards, procedures and guidelines on IPR compliance, and to investigate and prosecute third parties (especially Legal Department);
- Costs of purchasing additional software licenses, negotiating patent usage rights *etc*. where necessary to bring us into compliance;
- Costs for software license management activities – configuring and maintaining the software license inventory, conducting reviews of installed software, implementing license management systems *etc*.;
- IPR incident management and resolution costs *e.g*. legal defenses, fines, compensation;
- Diffuse costs resulting from a slightly more complex information security controls framework *e.g*. additional support calls to IT Help/Service desk relating to software licenses.

Control benefits

The benefits of good IPR controls include:

- Reduced IPR incident costs, fines *etc*. resulting from third party action against us, relative to the level expected if the controls were not effective (we may be able to use historical IPR incident costs, fines *etc*. as a guide to demonstrate the value of control improvements);
- Increased recovery from IPR action against third parties, license income *etc*., again relative to previous levels;
- Intangible benefits such as more understanding of our IPR risks and greater management confidence in our IPR controls (see below);
- Diffuse benefits such as a better understanding of our information assets plus a more comprehensive and reliable inventory.

Management confidence metrics

Management confidence in our IPR controls may be assessed using survey questions along the following lines. We anticipate conducting surveys periodically, quite likely combining these questions with other similar survey questions:

How confident are you that we take sufficient steps to uphold the intellectual property rights of third parties? Please mark the following percentage scale at the appropriate point, in your opinion.

0% 50% 100%

|----------+----------|

| | |

Not at all. Not quite enough >< Just about enough Absolutely!

We are almost certainly We are almost certainly

not in compliance with IPR fully compliant with IPR

requirements such as copyright and patents requirements and laws

Comments *e.g.* what led you to this score? Have there been particular situations or incidents that influenced your decision?

How confident are you that we take sufficient steps to protect and defend our own intellectual property rights? Please mark the following percentage scale at the appropriate point, in your opinion.

0% 50% 100%

|----------+----------|

| | |

Not at all. Not quite enough >< Just about enough Absolutely!

It is highly likely that third It is highly unlikely that third

parties are contravening our IPR parties are contravening our IPR

Comments *e.g.* do you know of any incidents in which our IPR was challenged, abused or stolen by third parties?

It is a simple matter to measure percentage values from each response and calculate the mean score. Provided enough survey forms are completed (ideally more than 30), the results should be statistically valid. The comments can provide useful feedback and quotations for use in management reports and other awareness materials.

Reporting

The financial metrics can be integrated into existing financial reporting. The other metrics may be reported periodically by the Information Security Manager to the Information Security Management Committee – we suggest quarterly for the first year (giving the metrics and controls time to settle down) and annually thereafter. In time, they may be integrated into the Information Security Management System Reporting Dashboard.

Conclusion

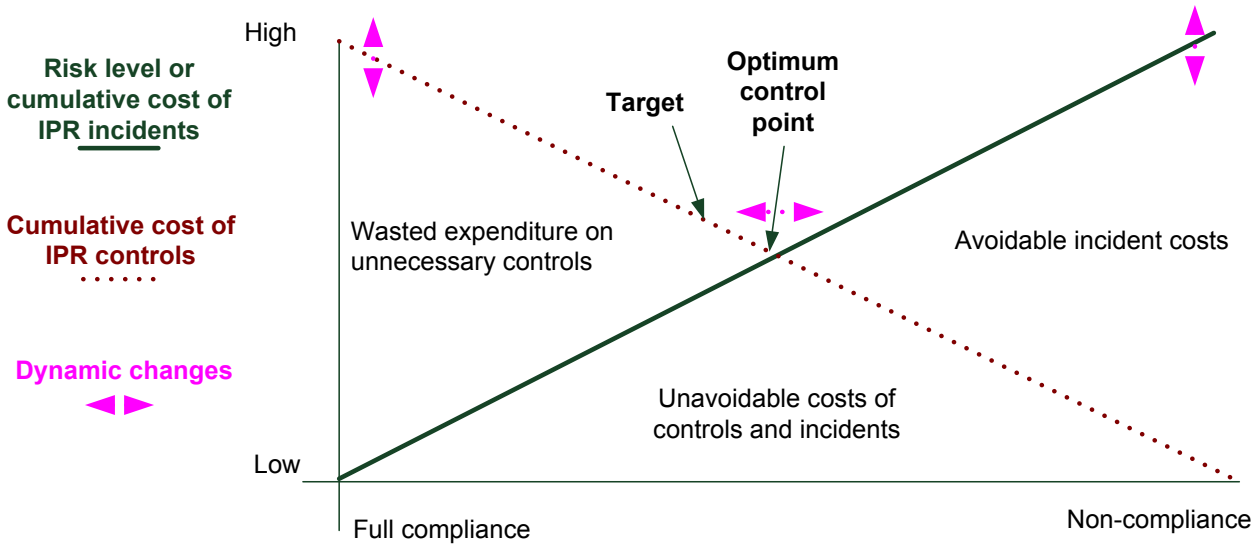
The metrics and reporting methods noted in this paper have hopefully stimulated you to derive creative and useful measures for your own situation. Do not neglect the value of having someone present and discuss reports with management. The dialogue that ensues can be very effective at teasing out any underlying issues and concerns on both sides. Why not present and discuss these ideas with your management and seek their opinions, bringing to the table some prototype reports in one or more formats to stimulate discussion and clarify their objectives? Better that than to prepare your reports blindly with no idea whether it is even read, let alone useful for management.

For more information

Please visit the information security intranet website for further information. Additional security awareness materials and advice on IPR are available on request from the Information Security Manager. NIST's Special Publication 800-55, a 99-page "Security Metrics Guide for Information Technology Systems" includes an extraordinarily comprehensive list of possible metrics and ISO 27004, a new international standard for information security management measurements, is currently being drafted by ISO with an anticipated release during the year ahead.

Appendix A

Diagrammatic representation of IPR risk-control tradeoff



Notes:

- We know it is difficult to measure the costs of incidents and controls or the level of risk in reality. As a diagrammatic representation, we are using the graph to illustrate the paper. It is not a strict academic model.
- It could be argued that the relationships are non-linear. For example, if one company is successful at suing us for damages over IPR non-compliance, adverse publicity might induce others to sue us also, exponentially increasing the risk and our costs. Similarly, the costs of achieving full compliance are likely to rise markedly as we meet and then exceed accepted best practices in this area.
- The target point is shown erring slightly on the side of caution, partly due to the uncertainties in this assessment and partly due to ethics.