

# Top 10 Tips for Incident Analysis

Prepared by Brian McIlravey, CPP  
Vice-President, Professional Services & Business Development, PPM 2000 Inc.

10

## **Answer the basics!**

Before you can do any sort of analysis, you need to accurately record the relevant information. Document what happened, when it happened, where it happened, why it happened, who was involved and how much was lost. Then, be consistent with your documentation across the board. With proper policies and procedures in place at the front end, you go a long way to ensuring accurate and meaningful analysis at the back end.

9

## **Share security information enterprise-wide.**

The more data you have, the more you can cross-reference and compare, and the more meaningful your conclusions will be. There's tremendous value in going beyond one location, or one department, to get an enterprise-wide understanding of your incident and investigation activity. Appreciating the sensitivity of this information, the most effective Incident Management systems allow you to segregate your data at various levels with some users restricted from reviewing (or analyzing) incident activity beyond their locations while others are granted access across the board.

8

## **Track costs... including losses and recoveries.**

When it comes to analysis, numbers talk... especially when they involve dollar signs. For example, one of the first steps in the risk assessment process is the creation of a Loss Event Profile. It shows the incident that has occurred (the threat) and how much that incident costs your organization each time it happens (impact in dollars). Without a proper tracking system, generating a Loss Event Profile can be difficult... or impossible. Conversely, with an effective Incident Management system, you can roll accurate incident data right into your security risk assessment program.

7

## **Set yourself up to easily perform analysis and quickly generate reports.**

As you track incidents, you generate data. Then, to effectively analyze this data, you need to correlate it. This can be tricky and time-consuming, especially if you want to perform analysis across multiple parameters... say, for example, location, date and classification. Doing it manually is almost impossible, and automated systems do it to varying degrees. Ensure that your system meets your analytical needs to minimize, or eliminate, any manual manipulation of the data.

6

## **Consider the investigative relevance.**

Data mining, investigative queries... you need the power to determine who was involved and when, how something happened and why. Spend some time analyzing for investigative facts. Scan your results for recurring patterns, names or other investigative details that may help solve an open case.

[continued...](#)

# 5

## **Measure current performance against past performance.**

Are we doing better, or worse, than last year? How do November's numbers compare with December's? In order to compare this year versus last year, or November 2007 with December 2007, you need to know what happened in the past—you need to be able to easily pull up that data, have the flexibility to work with any time frame and be able to clearly illustrate upswings or downturns. For this type of analysis, numbers are great... but graphs and charts speak volumes.

# 4

## **Address operational effectiveness and defend your budget.**

You need to allocate resources based on known issues, and you need to place the appropriate countermeasures against recurring problems. But, first, you need to justify the funds. Take the time to produce reports, graphs and statistics that demonstrate the effectiveness of your security department and your contribution to the bottom line. Then, present how you can become even more effective with additional investments in capital, operational or human assets.

# 3

## **Support knowledge-based decisions with hardcore statistical evidence.**

Spotting trends, tracking losses and threats, sharing information, performing analytical queries and generating graphical reports... all of these activities help you make knowledge-based decisions, decisions that are backed by evidence, justified by real numbers and more readily accepted by management. Statements based on "I think" and "I believe" only get you so far... give them something they can't argue with... give them hardcore statistics.

# 2

## **Focus on pattern analysis and trend spotting.**

So, what types of information should you routinely "analyze"? One thing that you should frequently watch for is patterns and trends. What do your incidents have in common? Is it the time... the location... an employee? After all, when you can identify a common element, you can do something about it. Commit some time to reviewing your incident records and to running routine analyses that look for common threads... sometimes you'll be surprised at what you see. Even an obvious pattern can be easily missed if no one takes the time to look for it.

# 1

## **Use your results to assess, manage and mitigate risk.**

The threat assessment process requires that you have access to previous history or reference to "empirical data." And, in order to mitigate risk, you need to know what threats are occurring, how often they occur, where they are occurring and how much they cost you each time they happen. With effective incident documentation, you lay the foundation for knowledge-based decision-making, and you have the tools necessary to spot trends and measure performance... all of which assist you in the risk mitigation process.

### **Effective Incident Analysis + Knowledge-Based Decision Making = Risk Reduction**

More than anything, effective incident analysis takes time... so spend your time in the most productive way possible. Let someone else, or something else, do the legwork so that you can focus on reviewing the results. The knowledge you gain will lead to better, more effective decision-making, and you'll benefit from an easier way of illustrating the return on your security investment.

Visit [www.ppm2000.com](http://www.ppm2000.com) to learn more about PPM 2000's Incident Management software solutions.



**PPM 2000 Inc.**  
10088-102 Avenue, Suite 1307  
Edmonton, Alberta T5J 2Z1

**www.ppm2000.com**  
information@ppm2000.com  
1-888-776-9776