

# SECURITY INFORMATION MANAGEMENT— THE FOUNDATION OF ENTERPRISE SECURITY

All organizations must be concerned about incidents and loss—a knowledge-based security program provides the best defense.

By Brian McIlravey, CPP





# Contents

Executive Summary	5
Introduction	7
Finding Information in a Big Corporate World of Data	8
The World of Security Data	9
The Roles of Incident Management & Risk Assessment	10
The Deming Cycle	11
The Six Questions	14
Documenting the Right Data	15
Transforming Data into Information	20
Generating the Right Reports	20
A New Age of Security Incident & Information Management	23
The ROI of Data-Driven Security	25
Conclusion	26
About the Author	28
About PPM 2000 Inc.	29
Incident Management from Every Angle Featuring Perspective by PPM 2000™	30



# Security Information Management— The Foundation of Enterprise Security

All organizations must be concerned about incidents and loss—a knowledge-based security program provides the best defense.

By Brian McIlravey, CPP

## Executive Summary

The management of ongoing incident activity is an inevitable reality for all organizations. Detailed information about what is going on within and across an organization's operations enables deployment of effective security safeguards that help reduce incidents and losses, and provide a built-in defense against accusations of negligence or inadequate security. However, gathering and extracting the right information from the mountains of data available is one of the most common challenges facing organizations today. This challenge can be easily overcome with the aid of powerful and sophisticated incident reporting and investigation management software solutions.



# EXTRACTING THE TERMS

## Introduction

All organizations face potentially serious consequences from incidents of all nature. These include losses and disruptions caused by the events themselves, as well as subsequent litigation and lost opportunity costs. The chronic occurrence of even relatively minor incidents can undermine an organization's culture, cohesiveness and reputation. And in the extreme, major incidents can bring literal ruin to an organization. For instance, in 1995, fraudulent trading to the tune of \$1.4 billion by rogue trader Nick Leeson forced the renowned British Barings Bank into bankruptcy. This cost 4,000 employees their jobs and huge losses for investors. Leeson, who worked out of the bank's Singapore office, was later convicted and sentenced to six and a half years in prison.

*While incidents and losses can never be totally prevented, an organization's visible commitment to knowing what is happening on its premises, in its surrounding neighborhoods, and across its operations is critical.*

Using information about actual and prevented incidents is essential to the development of effective security safeguards for each workplace environment, and a demonstrable commitment to collecting and constructively acting on this information is at the heart of successful litigation outcomes when the prosecution argues that the defending organization could have foreseen and prevented incidents from occurring.

Unfortunately, the collection, analysis and management of incident data does not happen by itself; it is the Achilles heel of most security programs. This weakness includes failure to:

- Collect incident data in a consistent and accurate manner.
- Store and proactively manage this data.
- Secure the data from unauthorized access and potential corruption.
- Analyze the data to derive useful information about security issues, as well as to educate upper management about the variety and intensity of threats that their organizations face.
- Act on the analytical information gleaned from the data in order to reduce or prevent incidents and loss.

While the scene is changing dramatically in the age of the CSO (Chief Security Officer) and numerous management programs dedicated to security, it is surprising that many security

*The following terms appear throughout this whitepaper and are listed here in alphabetical order for your reference.*

### Annual Loss Expectancy

The expected total loss value attributed to a particular type of event for one year. Calculated by multiplying the expected frequency of the event for a one-year period (the number of times it will likely occur in a year) by the event's single loss expectancy (the loss value of the event occurring once).

$$\text{Annual Loss Expectancy} = \text{Frequency} \times \text{Single Loss Expectancy}$$

### Benchmark

A point of reference against which something can be measured. Also referred to as a baseline measurement.

### Countermeasure

A protective measure (physical or procedural) put in place to either minimize the frequency of an event or its impact.

# EXTRACTING THE TERMS

operations still depend on inefficient office automation and reporting practices for incident management. For example, a number of corporate security departments have abandoned paper-based incident reports and conventional filing systems in favor of home-grown electronic incident reporting systems. While more efficient than paper reports, these electronic flat files are no more effective than traditional filing cabinets. They are searchable only with great effort, and they make finding specific information, doing analysis and generating reports very time-consuming. This is quite remarkable—and fast becoming unacceptable—with the need for immediate information and business intelligence in this day and age of fast-paced commerce and powerful threats and vulnerabilities.

Most organizations would say that they are, quite literally, drowning in data—while still suffering from a chronic lack of information on which to base decisions. This picture is not acceptable and it must change in order to maintain an effective risk management program.

## Finding Information in a Big Corporate World of Data

The business world today is a data-centric world. Decisions based on carefully analyzed data are not only more likely to be correct and bring results, they are also more readily accepted and trusted. The term “knowledge-based decisions” is gaining currency. It refers to the knowledge and insights that are gleaned from raw data.

As stated earlier, most corporations today are flooded with data, so much so that virtually no one in a typical corporation has the “big picture” of what is really going on. Ironically, that has become the convenient defense of executives involved in some recent high-profile corporate scandals. Yet, there is a recognizable truth lurking in and around their arguments; it should be understandable that there was much they did not know. One hears the same argument from all directions. Much data, but not enough clear information. Too many issues to track and understand, and not enough confidence that the grounds for action are valid or, if valid, an unwillingness to incur the expense of correcting the situation.

There is an obvious need for reliable business intelligence to drive actions. The challenge—and the obvious, if daunting, opportunity—is that our world of data is growing exponentially and becoming even more complex.

It is only over the last two decades or so that organizations and

### Deming Cycle

A cyclical management process designed to solve issues and improve procedures and responses. Also referred to as the PDCA cycle (Plan, Do, Check, Act).

### Event

An occurrence, either accidental or purposeful, caused by human or natural factors.

### Frequency

The number of times an event has occurred over a span of time. Also referred to as the likelihood or probability of the event’s occurrence.

### Impact

The measured effect of an event on an organization. Also referred to as the consequence of the event. May be tangible or intangible, with or without an associated dollar loss value.

### Incident Management

The process of identifying and analyzing incident activity and determining the best course of action for handling it, presently as well as in the future.

# EXTRACTING THE TERMS

their software suppliers have begun to focus on the challenge of how to make sense and use of the mountains of data available to them. Data storage, data management and data mining are now huge businesses for IT suppliers and consulting firms. Likewise, the emerging field of data and business analytics is providing sophisticated tools, algorithms and modeling techniques to draw from raw data meaningful analysis, knowledge and predictive studies that provide guidance on strategy and future investment.

## The World of Security Data

Progress must still be made in the practical integration of data management technology into daily security operations. Industry surveys show that security managers rank “office management” and paperwork as one of their most serious time consumers and sources of inefficiency. Budget preparation and justification is also a predictably large, and mostly unpleasant, time consumer. Even worse are one-off requests from upper management that invariably wreak havoc on a normal work week. The new trends of performance measurement and performance management now add an even greater degree of required reporting from pre-determined metrics and measures.

The world of security data is fundamentally disorderly, primarily because there is no obvious—let alone easy and convenient—way to organize a substantial variety of seemingly disparate data. It is for this reason that so little security department data is well utilized, even if it is routinely collected and archived. Some security directors will admit that very little of their data is routinely scrutinized for the identification of patterns and trends and for making decisions about logical corrective action. This, of course, changes decidedly in the days and weeks following a high-visibility incident when 20/20 hindsight becomes very apparent. Security directors explain that the lack of qualified data analysts and the time demands placed on management result in reactive “management by red flags”—which means responding to crises rather than developing proactive, data-based security strategies.

It is absolutely critical for security departments to realize that the amount and variety of security data flowing into their information systems is only going to grow—day-by-day and year-by-year—both as their corporations grow and as new technology-based security systems come on line. The corresponding need to store and organize this data for meaningful use will thus become an ever more pressing issue that will almost certainly command more upper management interest and scrutiny.

### Loss

The resulting impact of an event. Losses are usually measured in dollars, though intangible losses may also result from incident activity (e.g., loss of corporate reputation).

### Risk

“The likelihood of damage or loss [associated with an event’s occurrence] multiplied by the potential magnitude of the loss.”<sup>1</sup>

### Risk Management

“The process of determining whether or how much of the risk [associated with an event’s occurrence] is acceptable and what action should be taken.”<sup>2</sup>

### Security Information Management

The collection, storage and management of security data for analysis of patterns, trends, potential risks and other intelligence.

### Single Loss Expectancy

The expected loss value of an event occurring once.

### Threat

An event that can potentially occur.

---

<sup>1</sup> Garcia, Mary Lynn. (2001). [The Design and Evaluation of Physical Protection Systems](#). Woburn, MA: Butterworth-Heinemann.

<sup>2</sup> McNamee, David. (1998). [Business Risk Assessment](#). Altamonte Springs, FL: The Institute of Internal Auditors.

[Click here to request the complete White Paper.](#)