WHITE PAPER

by Brian McIlravey, CPP
and Peter Ohlhausen

Strengthening Intelligence and Investigations with Incident Management Software

About the Authors:

Brian McIlravey, CPP, is Co-CEO of PPM 2000 Inc. (www.ppm2000.com). He is a member of ASIS International's Information Security Technology Council and has experience in both corporate security and public law enforcement.

Peter Ohlhausen is president of Ohlhausen Research, Inc. (www.ohlhausen.com), which for more than 20 years has provided research and consulting to the security, technology, and criminal justice fields. He formerly served as editor of *Security Management*, the monthly magazine of ASIS International.

Published by PPM 2000 Inc.
www.ppm2000.com

PPM 2000 helps organizations meet their risk, performance and intelligence objectives with Incident Management solutions that leverage technology and process for a powerful knowledge base. Perspective by PPM is an end-to-end software solution for responding to, reporting on and analyzing enterprise security events. Users intelligently action and query their data to make informed decisions that reduce risk, optimize performance and illustrate the effectiveness of their security and investigative operations.

For more information on incident management—and on Perspective—contact PPM toll-free at 1-888-776-9776 or email information@ppm2000.com.

Contents

Executive Summary 7

Introduction 8

Trends Calling for Software Use in Intelligence and Investigations 9

- Big Data 10
- Metrics 11
- Excellence 12
- Enterprise Security Risk Management 13
- Standards 15

Using Software for Intelligence and Investigation 16

- Apply the PDCA/Deming Cycle 17
- Master Analytical Competencies 18
- Build and Mine the Data Set 19

Moving Forward with Analytics 22

References 23

PPM 2000 Inc.

10088 - 102 Avenue, Suite 1307 • Edmonton, Alberta • T5J 2Z1

1-888-776-9776 • 1-780-448-0616 • information@ppm2000.com • www.ppm2000.com

Executive Summary

Incident management software, and the data collection and analysis that the software supports, serves three primary purposes: (1) risk management; (2) performance management; and (3) intelligence and investigations.

Prior papers focused on the first two topics. "Security Information Management—The Foundation of Enterprise Security" (McIlravey, 2009) addressed risk management, and "Metrics and Analysis in Security Management" (McIlravey & Ohlhausen, 2012) addressed performance management. This paper emphasizes the third purpose, intelligence and investigations, and discusses how the right incident management and analytical software can empower security professionals in their efforts to discover and understand information and connections *(gain intelligence)* and act on *(investigate)* security incidents that affect their organizations.

Several high-level business trends encourage the use of software for intelligence and investigative purposes, including: big data, metrics, excellence, enterprise security risk management and standards. Software-empowered intelligence and investigations is consistent with these trends and, in some cases, essential for participating in them.

With a widely sourced database and the appropriate software, analysts and investigators can reduce guesswork by revealing complex associations hidden in the data; display routine data as visual elements that are easy to analyze and interpret; quickly navigate the data to identify additional relationships; and process large volumes of data into actionable intelligence that brings clarity to complex investigations and scenarios.

Security professionals employing incident management and analytical software apply the Deming Cycle where they Plan-Do-Check-Act. They master analytical competencies, such as information management, analytics skills and tools and data-oriented culture. And, using these competencies, they build the data set and transform it into intelligence through data mining, link analysis, timeline charting, pattern analysis and trend spotting. As a result of these efforts, their organizations are in a better position to discover, prevent and solve security incidents and crimes.

The paper concludes with recommendations on moving forward with a software-based intelligence and investigation program. Steps include assessing current analytics sophistication, improving analytics competencies and developing an information agenda.

Introduction

Incident management software, and the data collection and analysis that the software supports, serves three primary purposes:

- Risk management
- Performance management
- Intelligence and investigations

Prior papers focused on the first two topics. "Security Information Management—The Foundation of Enterprise Security" (McIlravey, 2009) addressed risk management, and "Metrics and Analysis in Security Management" (McIlravey & Ohlhausen, 2012) addressed performance management. This paper emphasizes the third purpose, intelligence and investigations.

The right incident management and analytical software can empower security professionals in their efforts to: (1) discover and understand information and connections *(gain intelligence)*; and (2) act on *(investigate)* security incidents that affect their organizations.

Investigative analysis centers on the intelligence cycle—the continuous collection and analysis of timely data related to an investigation. Data sources may be singular (e.g., incident reports stored in an incident management tool such as Perspective by PPM) or multiple (e.g., incident records plus communication and transaction records plus public, open-source data). To make informed decisions and take actions based on facts, a security professional must be able to quickly and effectively track and analyze data. Doing so requires a comprehensive range of visualization and analytical tools that deliver intelligence by finding connections, patterns and trends in complex data sets.

It is one challenge to collect and organize vast amounts of data. It is another to derive actual information from that data. In the course of a security investigation, it may be necessary to find a needle (a useful fact) in a haystack of data. Often investigators find that the answer to their question is already in their data set, but where? How can they move from small insights to seeing the big picture?

Movies and television programs often show investigators tacking photos, receipts, maps and other data items to a board, then linking the elements with strings to show connections. The

SOFTWARE: A KEY TOOL IN SECURITY'S VALUE STREAM

A Value Stream is a collection of processes designed to achieve a result for an internal or external customer…. A Value Stream for information within an organization is… a cascading waterfall moving from data aggregation derived from process outputs, devices, software, databases, human and other organizational assets….

Information must be organized… to be easily searched and found. Analytics must be applied within the context of time, metrics, and comparative sources to create the opportunity to drive intelligence. Intelligence drives strategic and tactical responses.

The Value Stream of Security (Worman, 2012)

directors might as well show libraries with card catalogs or clerks keeping a firm's books with quill pens. It is archaic and infeasible to discover key connections between data bits in such a slow, analog manner. Security professionals now use investigation-focused software to discover those key connections, to find the needle in the haystack.

This paper, based on a review of the literature as well as interviews with security professionals, first looks at high-level business trends that encourage the use of software for intelligence and investigative purposes. The paper then describes how security professionals are building diverse, inclusive data sets and using security-focused incident management and analytical software to identify connections that help in discovering, preventing and solving security incidents and crimes. The paper also examines techniques currently in use among security professionals, such as investigative data mining, link analysis, timeline charting, pattern analysis and trend spotting.

In brief, the paper examines why a security professional should collect data and use it to the fullest, and it offers a concise, high-level look at how to do so. Sections include:

- Trends Calling for Software Use in Intelligence and Investigations
- Using Security Software for Intelligence and Investigations
- Moving Forward with Analytics

Information security management *refers to protecting information.* ***Security information management*** *means the management and organization of data, leading to quantitative and qualitative results.*

Trends Calling for Software Use in Intelligence and Investigations

Several current business trends would seem to encourage the use of: (1) inclusive databases; and (2) management or analytical software. Those trends or developments include the following:

- Big data

DATA-DRIVEN DECISIONS

The evidence is clear: Data-driven decisions tend to be better decisions. Leaders will either embrace this fact or be replaced by others who do. In sector after sector, companies that figure out how to combine domain expertise with data science will pull away from their rivals. We can't say that all the winners will be harnessing big data to transform decision making. But the data tells us that's the surest bet.

Big Data: The Management Revolution
Harvard Business Review
(McAfee & Brynjolfsson, Oct 2012)

- Metrics
- Excellence
- Enterprise Security Risk Management
- Standards

Software-empowered investigation and intelligence development appears to be consistent with these trends and, in some cases, essential for participating in them. Intelligence and investigations require sophisticated data collection and use; these trends do the same.

Big Data

The concept of "big data" is much discussed in the business literature. Researchers and business people remark on the gigantic volume of business data now available and speculate on how best to make use of it. For example (Brown, Chui & Manyika, 2011):

> Over the last few years, the volume of data has exploded. In 15 of the US economy's 17 sectors, companies with more than 1,000 employees store, on average, over 235 terabytes of data—more data than is contained in the US Library of Congress. Reams of data still flow from financial transactions and customer interactions but also cascade in at unparalleled rates from new devices and multiple points along the value chain....
>
> All of this new information is laden with implications for leaders and their enterprises. Emerging academic research suggests that companies that use data and business analytics to guide decision making are more productive and experience higher returns on equity than competitors that don't.

The authors note a study (Brynjolfsson, Hitt & Kim, 2011) that found that effective use of data and analytics correlated with a 5 to 6 percent improvement in productivity, as well as higher profitability and market value.

Big data is not merely discussed but, more and more, is being implemented. A survey of 1,469 C-level executives by global management consulting firm McKinsey & Company found a high level of emphasis on the use of big data. Of the three business technology trends the survey asked about, more than half of respondents reported that their organizations have made "big data and analytics" a top-ten corporate priority on their strategic agendas.

DAUNTING DATA

One key area of advanced technology still emerging is management of data. As technology increases, so does the amount of data derived from systems.... Accumulating this data, assessing it, and making use of it, especially in terms of pulling out alarms and alerts that could indicate a security problem, is a daunting task. Managing "big data" is a very big problem. Advanced analytics, advanced security incident management, risk management, intelligence software, and other applications are being developed and integrated at a very fast pace to meet this need.

Utilities Critical Infrastructure Protection: Security Dependencies and Trends (ASIS Utilities Security Council, 2012)

Of special interest is the widening scope of data sources. In the *Harvard Business Review*, Barton and Court (2012) expand on the implications of collecting a wide range of information and making use of its value:

> The universe of data and modeling has changed vastly over the past few years. The sheer volume of information, particularly from new sources such as social media and machine sensors, is growing rapidly. The opportunity to expand insights by combining data is also accelerating, as more-powerful, less costly software abounds and information can be accessed from almost anywhere at any time. Bigger and better data give companies both more-panoramic and more-granular views of their business environment. The ability to see what was previously invisible improves operations, customer experiences, and strategy. But mastering that environment means upping your game, finding deliberate and creative ways to identify usable data you already have, and exploring surprising sources of information….
>
> Managers also need to get creative about the potential of external and new sources of data. Social media are generating terabytes of nontraditional, unstructured data in the form of conversations, photos and video. Add to that the streams of data flowing in from sensors, monitoring processes and external sources that range from local demographics to weather forecasts.

Metrics

As noted earlier, this paper continues a treatment begun in an earlier paper, "Metrics and Analysis in Security Management" (McIlravey & Ohlhausen, 2012). That paper provided a baseline definition of metrics from Carnegie Mellon University (1995):

> [M]etrics are quantifiable measurements of some aspect of a system or enterprise…. Security metrics focus on the actions (and results of those actions) that organizations take to reduce and manage the risks of loss of reputation, theft of information or money, and business discontinuities that arise when security defenses are breached.

Current research on security metrics expands the scope of the Carnegie Mellon definition and examines the full range of security risks.

The paper then describes security professionals' use of metrics, sometimes called analytics, to improve decision making, strengthen security operations and gain support for the security and risk management operation.

"Bigger and better data give companies both more-panoramic and more-granular views of their business environment. The ability to see what was previously invisible improves operations, customer experiences, and strategy. But mastering that environment means upping your game, finding deliberate and creative ways to identify usable data you already have, and exploring surprising sources of information…."

(Barton & Court, 2012)

The concept of using data from various sources to develop intelligence and improve investigations fits well within a broader corporate interest in metrics or analytics. A study by the *MIT Sloan Management Review* and the *IBM Institute for Business Value,* "Analytics: The Widening Divide" (Kiron et al., 2011), found that 58 percent of responding organizations use analytics to create a competitive advantage. Those same organizations were reportedly more than twice as likely to substantially outperform their peers. The study report noted:

> With the digitization of world commerce, the emergence of big data and the advance of analytical technologies, organizations have extraordinary opportunities to differentiate themselves through analytics. The majority of organizations have seized these opportunities....
>
> We closely examined what the transformed organizations, the most sophisticated users of analytics, are doing well and found three key competencies: (1) information management, (2) analytics skills and tools, and (3) data-oriented culture. Mastering these competencies enables organizations to gain full benefit from analytics....
>
> Analytics confers greater agility, acuity and certainty in today's fast-changing business environment.

A study by the MIT Sloan Management Review and the IBM Institute for Business Value, "Analytics: The Widening Divide" (Kiron et al., 2011), found that 58 percent of responding organizations use analytics to create a competitive advantage. Those same organizations were reportedly more than twice as likely to substantially outperform their peers.

Within the security field, an emphasis on metrics continues. At the 58th Annual ASIS Seminar and Exhibits in 2012, the Metrics Working Group of the ASIS Defense and Intelligence Council gave a presentation titled "Build an Effective Security Performance Metric." It named a wide range of data that security professionals should collect, such as the level of shrinkage; number of workplace violence incidents; number of outages due to vandalism; dollar value of fines, judgments, and penalties due to security or safety issues; and numbers of particular assets, such as desktop computers, laptops, mobile devices, production servers, etc. Intelligence/investigative use of data likewise relies on the collection of a wide range of data sources.

Excellence

In the business world generally, over the last several decades, the concept of excellence has influenced business practices and led to the development of such excellence-oriented strategies as Six Sigma, Kaizen, Operations Excellence and Total Quality Management. As a business practice, excellence uses quality management principles and tools to improve performance. Among

the key practices in business excellence are continuous and breakthrough improvement and management by facts.

Currently a group of security professionals is working to define how the practice of excellence applies to the security field. Campbell (2012) writes, "There is no shared definition of excellence, quality or other key performance measures that would facilitate common, cross-industry benchmarks for security." A report by the Security Executive Council (2012) notes that the council is working to address that deficiency by developing a "Business Excellence Tool Kit." The group hopes to "put forth a body of workable definitions for various security activities, provide measures and metrics appropriate to assessing performance and service quality and craft tools and templates that will support the pursuit of documented excellence."

The report presents a business excellence template designed to help security teams identify the benefits of an "in-depth application of an operations excellence approach." The table leads users to think about how to obtain business-responsive results from investigations through the use of best-in-class security practices and improved responsiveness to key risk indicators. Both of those techniques rely on the collection and use of data by security professionals.

Enterprise Security Risk Management

The concept of enterprise security risk management (ESRM), currently promoted by many in the security field, aims to include new and developing security concerns into the universe of risks that an organization considers. A report by ASIS's CSO Roundtable (2010), based on a survey of chief security officers, observes:

> Years ago, ASIS began reaching out to other security associations... to create an integrated approach to identifying and mitigating all the risks that organizations face. This effort was dubbed enterprise security risk management—ESRM. With ESRM's holistic approach to security came the understanding that a whole host of business issues that were not traditionally associated with "security"—think, for example, of Sarbanes-Oxley or HIPAA—were now firmly part of security's bailiwick, underscoring again how important it is for security professionals to be business professionals first....
>
> [ESRM] is a vital element of Enterprise Risk Management (ERM), which examines the universe of risks—financial, strategic, operational, legal, accidental, and so on—that an organization faces.

OPERATIONS EXCELLENCE

If enterprise security is to be effectively aligned with its company's strategy and processes, it must be driving a focus on operations excellence (OpEx) into every corner of its suite of products and services.

(Security Executive Council, 2012)

> But where ERM has typically been associated with the financial side of business—such as credit risk and commodities-pricing risk—ESRM highlights the protection of assets and activities such as physical security, investigations, crisis management, business continuity, and data protection. Any disruption in one of these areas could be as harmful to an organization's profit or reputation as a hedge-fund investment or currency-exchange practice.

ESRM requires paying attention to several key issues related to data-based intelligence and investigations. Security professionals need to consider optimal software use, range of data collected and potential litigation avoidance benefits.

Optimal Software Use

CSO Roundtable survey respondents noted that the first step in making sure ESRM efforts are efficient is to "determine what types of data need to be aggregated and analyzed." One CSO said, "From the tactical level, part of it is your whole case management system; part of it is your financial reporting tools; and then pulling them all together in terms of a dashboard." He noted that incident management tools (such those from PPM) have helped him manage physical and information security incidents. He recommended aggregating data into "dashboard-views of the world."

Range of Data Collected

In "The New Enterprise Security Risk Manager," a presentation at the 58th Annual ASIS Seminar and Exhibits, Slotnick (2012) lists numerous types of data sources that security professionals should tap:

- Physical access control systems (PACS)
- Video surveillance
- Communication interoperability platforms
- Incident reporting
- Door technology
- Video management
- Voice-over-IP and radio-over-IP
- Identity management
- Video analytics
- Intercom
- Performance reporting (people, processes, technology)
- Intrusion detection
- Video storage and retrieval

Enterprise Security Risk Management (ESRM) highlights the protection of assets and activities such as physical security, investigations, crisis management, business continuity, and data protection. Any disruption in one of these areas could be as harmful to an organization's profit or reputation as a hedge-fund investment or currency-exchange practice.

(ASIS CSO Roundtable, 2010)

- Smart phones
- Forensics and prosecution

Despite his call for collecting a wide range of information, he states, "Complexity is not an answer," and he encourages the use of commercial off-the-shelf (COTS) software to manage the data collected.

Litigation Avoidance

Another ESRM connection to data-based investigations is the notion of having an unbiased origin for investigations in order to avoid litigation. Clark (2013) writes:

> Conducting corporate security investigations is risky business.... Litigation risk increases dramatically when any phase of the investigative process... is handled inconsistently....
>
> How a case originates is another area examined in a civil suit or criminal proceeding. The vast majority of a security department's investigations begin as tips or complaints. However, electronic tips derived from fraud analytics—the proactive detection of fraud and unproductive business through the analysis of data—can offer companies greater protection from frivolous law suits.
>
> The greatest benefit to deploying a fraud analytics strategy is that fraud profile results have no race, religion, sex, or sexual orientation. Profile results do not identify if the employee is high or low on the seniority list or how well they perform their job functions. Fraud profile results create the ultimate objective, non-biased and non-discriminatory electronic tip, identifying fraudulent or speculative activity requiring additional investigative work. Cases originating from a fraud profile will not prevent a suit from occurring... [but] will put your company and investigative team in the most defensible position.

Standards

The rise of security standards is another trend calling for the collection of a wide range of data and its use for intelligence and investigations. For example, the ASIS/ANSI *Chief Security Officer (CSO) Organizational Standard* (2008) calls for the use of data as follows:

> 6.3 Information Gathering and Risk Assessment
>
> The CSO is responsible and accountable for systematically gathering, assessing, and synthesizing information related to a

The CSO is responsible and accountable for systematically gathering, assessing, and synthesizing information related to a wide range of security-related events and threats specific to the organization and its various operations, which may adversely affect the security and safety of personnel and the profitability or reputation of the organization.

(ASIS Int. & American National Standards Institute, 2008)

> wide range of security-related events and threats specific to the organization and its various operations, which may adversely affect the security and safety of personnel and the profitability or reputation of the organization.
>
> In addition, the CSO should... determine the probability of security-related incidents and threats, and develop appropriate strategies... to prevent negative impacts on the organization. The information necessary to develop these assessments and preventive strategies should come from multiple sources, including organizational records, government and law enforcement (including intelligence) agencies, news organizations, existing security bodies of knowledge, etc. The CSO should be capable of making the links between disparate pieces of information, from multiple sources, in order to understand and assess the data's importance to the security of the enterprise. The CSO should... be familiar with... technological aids that can assist in this process.

Similarly, in their standard titled *Workplace Violence Prevention and Intervention* (2011), ASIS and the Society for Human Resource Management specify data-oriented steps for investigating workplace violence concerns. The standard calls for the investigation to dig into:

> workplace computers or networks, public records, databases, social media, and other sources legitimately available to the organization, for information pertinent to expressed hostilities, violent ideation, and a history of harassment, aggression, or violence.

Using Software for Intelligence and Investigations

In developing workplace intelligence and conducting investigations, security professionals try to make informed decisions and take actions based on facts. As noted in the previous section, several major trends in the business world and the security field are pushing them to do just that. Many security professionals are using incident management and investigative software to quickly and effectively track their investigative data and analyze it in search of meaningful patterns.

Many security professionals are using incident management and investigative software to quickly and effectively track their investigative data and analyze it in search of meaningful patterns.

In investigations, security professionals are generally looking for proof—that is, looking to develop a conclusion built on a foundation of facts. They collect a broad base of accepted information on which they can base other assertions relevant to the

investigation.

When the pieces of data do not fit together sufficiently to form an investigative narrative, picture or explanation, security professionals typically must start from scratch to build searches and queries to reassemble the proof and look for missing links. That approach is called a null-start, and in a null-start, investigators using a widely sourced database and appropriate software can do the following:

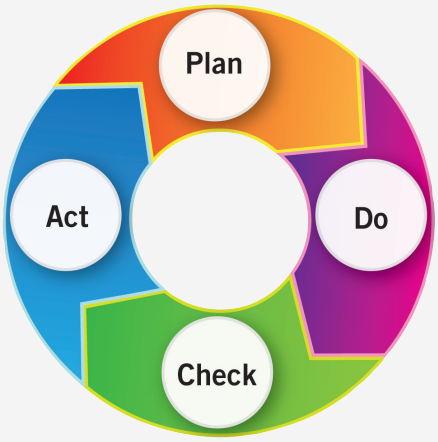
- Reduce guesswork by revealing complex associations hidden in the data.
- Display routine data as visual elements that are easy to analyze and interpret.
- Quickly navigate the data to identify additional relationships.
- Process large volumes of data into actionable intelligence that brings clarity to complex investigations and scenarios.

Apply the PDCA/Deming Cycle

Like certain other business processes, data-based, software-powered investigations can follow the Plan-Do-Check-Act (PDCA) cycle, also known as the Deming Cycle. It is named after W. Edwards Deming, who is often considered the father of modern quality control. It is a business management technique designed to support continuous improvement of processes and products, and it is based on the traditional scientific method. It includes the principle of iteration, calling on users to repeat the process once a hypothesis is confirmed or rejected to further extend their knowledge.

The PDCA cycle can be applied to intelligence and investigative work as follows:

- **Plan.** In this step, one carefully identifies the goal or target of the investigation and then collects data. Inputs should include a wide range of sources, such as customer relations management systems, enterprise resource planning systems, custom applications used by the organization, field contact cards, incident reports, activity reports, document control systems, radio frequency identification systems, and systems for alarms, closed-circuit television, access control, visitor control, and facility management. This step includes consolidating and harmonizing the data sets.
- **Do.** Here one visualizes and analyzes the data. Software



The Plan-Do-Check-Act (PDCA) cycle as it applies to intelligence and investigative work:

- **Plan.** Identify the goal or target of the investigation and collect data.
- **Do.** Visualize and analyze the data.
- **Check.** Disseminate the findings for review.
- **Act.** Take action based on the results of the three earlier steps.

makes it possible to perform relationship mapping, produce timelines, and discover obvious and non-obvious relationships.

- **Check.** At this stage, the security professional disseminates the findings for review. This step is also sometimes called "study" to emphasize the importance of analyzing the findings. By sharing the findings with other divisions of the organization, the security professional creates an opportunity for collaboration. Others can then contribute to the investigation, potentially by offering data sources that had not been included up to that point.
- **Act.** Here one takes action based on the results of the three earlier steps. If the findings were sufficient for the investigation, the action may be to move forward with termination or prosecution. If the findings were not yet sufficient, it is time to repeat the cycle, starting again with the planning step, and to continue the cycle until the required intelligence or investigative information is discovered.

Master Analytical Competencies

Research published in the *MIT Sloan Management Review* (Kiron et al., 2011) found that to achieve sophistication in the use of analytics (another term for data-founded intelligence development), organizations typically master three competencies: information management, analytics skills and tools and a data-oriented culture.

Information Management

Companies skilled in information management are able to "capture, combine and use information from many sources,… [integrating] information across functional and business silos." This skill involves using a variety of techniques for managing data and developing a common data architecture, including standards for data quality across all business units and functions. Also vital is the ability to manage the data in real time.

Analytics Skills and Tools

The study found that "organizations that deploy new skills and tools for analytics can typically answer much harder questions than their competitors." Advanced analytical techniques also save time, "freeing individuals to apply data and insights to higher-level business questions, such as using analytics to detect fraud."

A CULTURE OF DATA

We have used exception reporting since the late 1990s. We use a couple of different products…, including software from our internal audit department…. For instance, we will take a list of all the addresses that we ship to via our shipping company and match them to our employee addresses, looking for employees who are getting lots of packages shipped from their stores.

Chris Hoffman,
Corporate Investigations Manager,
Bon-Ton Stores (2012)

Data-Oriented Culture

The Kiron et al. study in the *MIT Sloan Management Review* also found that analytical sophistication thrived in organizations with a data-oriented culture. Such organizations emphasize the principle that business decisions must be based on analysis of data. The study notes:

> Leaders within organizations that have mastered this competency set an expectation that decisions must be arrived at analytically, and explain how analytics is needed to achieve their long-term vision.
>
> In these data-driven cultures, expectations are high. Before "giving the green light" to a new service offering or operational approach, for example, leaders ask for the analytics to support it. They express their conviction in the value of faster and more precise decisions by using analytics to guide day-to-day operations. Employees are confident they have the information to make data-based decisions. They are encouraged to challenge the status quo, and follow the facts in order to innovate.

Build and Mine the Data Set

To get the greatest amount of intelligence from data, security professionals first maximize their data set, then analyze it. Specialized tools, such as incident management software and data analysis software, make advanced search and analysis feasible.

Maximize Data Set

Data is the fuel of the intelligence cycle—the more data an investigation has access to, the farther that investigation can go.

The desired quantities of data cannot be assembled, sorted, or comprehended through a manual system. Incident management software is a tool for capturing the who, what, when, where, why, how and how much from as wide a range of data as the security professional can obtain. For example, Perspective by PPM can do the following:

- Document events and provide structured incident reporting.
- Capture and sort important details on people, vehicles, organizations, items, evidence, narratives, notes and attachments.
- Harmonize data (by matching differently-entered forms of the same name, address or other data point).

INTEL AT DELTA

We collect many types of data: reports from employees; compliance reports; customer service information; damage reports; productivity figures; compliance issues; and data on accidents, emergencies, financial crimes, and crimes against persons. Then we analyze it so we can:

- Take specific steps to stop losses or crimes in specific locations (e.g., increasing screening); and
- Make policy recommendations to senior leadership (e.g., conducting employee training).

We have charted credit cards tied to ticket fraud tied to certain cities and then implemented better security and better software to reduce or prevent such fraud.

Kim Hodgkin,
Manager of Security Administration,
Delta Air Lines (2011)

- Help support and manage investigative process and cases.

Transform Data into Intelligence

At this stage, the security professional attempts to convert data into intelligence—that is, information of sufficient quality to make knowledge-based decisions. In general terms, the investigator is looking for proof to solve a puzzle. He or she may see the mass of data but have no way to link individual bits of data. In that case, the investigator does a null-start. If no available data can be linked to a person's name, it may help to try a search of the person's phone number or address. Once a linked data bit is discovered, the investigator tries to link that data bit to another data bit to create a picture that the investigator could not see before.

Software-based techniques for establishing links between bits of data include pattern analysis, link analysis and timeline charting.

Pattern Analysis

Incident management software can provide pattern analysis and trend spotting. For example, a person who has a known link to a security incident, and who is then identified by the software as having a pattern of trespassing in the past, may be a logical subject for further investigation. Patterns and links can also be discovered through triangulation. The same person identified above may be associated with another person, and both of them associated with an organization (such as a criminal organization or radical group). An investigator may then discover that the group is involved in various types of incidents (such as theft or fraud) and discern a pattern in which multiple people from the same group are involved in the incidents.

Link Analysis

Here one looks for obvious and non-obvious links, relationships or connections. An obvious connection might be that the suspect is a sibling of a company employee. A non-obvious connection might be found by comparing key parties' phone numbers and finding that they share a landline phone and hence may share a residence or office. Security software can often find such non-obvious connections even when the data items are spelled differently (e.g., 5th St. versus Fifth Street).

Graphics help in understanding the connections between bits of data. Using a tool like Perspective Visual Analysis, security

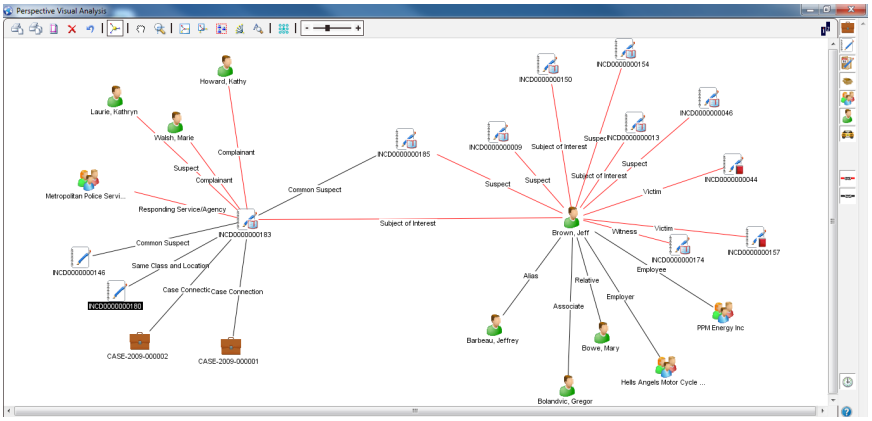
DATA'S PURPOSE: BETTER DECISIONS, DEEPER INSIGHTS

In their quest to extract insights from the massive amounts of data now available from internal and external sources, many companies are spending heavily on IT tools and hiring data scientists. Yet most are struggling to achieve a worthwhile return. That's because they treat their big data and analytics projects the same way they treat all IT projects, not realizing that the two are completely different animals….

Even when such projects improve efficiency, lower costs, and increase productivity, executives are still dissatisfied. The reason: Once the system goes live, no one pays any attention to figuring out how to use the information it generates to make better decisions or gain deeper—and perhaps unanticipated—insights.

Why IT Fumbles Analytics
Harvard Business Review
(Marchand & Pepper, Jan-Feb 2013)

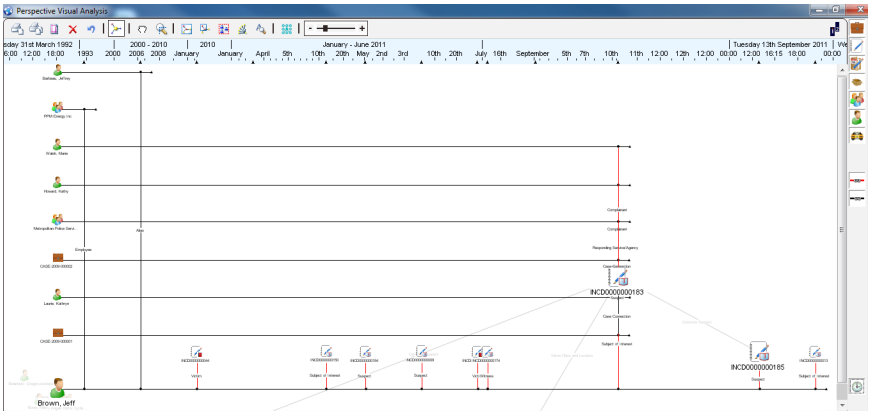
professionals can create visual elements that are easier to analyze and interpret than tables of data would be. In some cases, graphics can help an investigator visually triangulate an answer from seemingly unrelated events.



Perspective Visual Analysis

Timeline Charting

Another type of graphic is the timeline chart, which depicts a series of events pinned to a timeline in order of occurrence, while at the same time cross-referencing data (such as persons involved) to the timeline. The chart enables an investigator to view data in time-based measurement instead of relational measurement (aka the spider web chart). For example, as shown below, with time-based analytics, investigators could view a series of similar incidents over a large span of time and pinpoint a person who had been involved multiple times over the series of events.



Perspective Visual Analysis

Using a tool like Perspective Visual Analysis, security professionals can create visual elements that are easier to analyze and interpret than tables of data would be. In some cases, graphics can help an investigator visually triangulate an answer from seemingly unrelated events.

Moving Forward with Analytics

In "Analytics: The Widening Divide" (2011), Kiron et al. report on their survey of more than 4,500 business executives, managers and analysts in more than 120 countries. The study led the researchers to make the following suggestions for organizations wishing to begin or strengthen their use of analytics:

- **Assess current analytics sophistication.** Security professionals should assess how close they are to their vision of an organization "transformed by analytics." They are encouraged to convene colleagues from other organizational functions or lines of business to address analytics concerns, such as data sharing, and to explore business challenges that can be addressed by analytics.
- **Improve analytics competencies**. Depending on the organization's current level of analytical sophistication, the security professional may need to work on improving one or more of the key analytics competencies mentioned earlier: information management; analytics skills and tools; and a data-oriented culture.
- **Develop an information agenda.** Developing an "information agenda" puts a security professional in the best position to align the organization's information technology to the desired analytics strategy. The researchers note, "An information agenda provides the balancing mechanism for acquiring and developing capabilities across all three competencies and across the enterprise."

In summary, security professionals are using incident management and analytical software to discover information and make connections *(gain intelligence)* and to act on security incidents that affect their organizations *(investigate)*. They find patterns and trends in complex, multi-source data sets, and they use their findings to discover, prevent and solve security incidents and crimes. High-level business trends—including big data, metrics, excellence, enterprise security risk management and standards—encourage the software-empowered approach.

Security professionals employing incident management and analytical software apply the Plan-Do-Check-Act or Deming Cycle; master analytical competencies, such as information management, analytics skills and tools and data-oriented culture; and build a data set and transform it into intelligence. Specific

ANALYTICS MADE EASY AND POWERFUL

When I was in policing, conducting investigations, I would have loved a tool like Perspective. It's easy and powerful.

One of the most important functions of Perspective is its analytical capability. It helps us create actionable intelligence for investigations and operations.

Brian Tuskan,
Senior Director of Global Security Technology & Investigations, Microsoft Corporation (2011)

steps for starting or improving a software-based intelligence and investigation program include assessing current analytics sophistication, improving analytics competencies and developing an information agenda.

References

ASIS International and American National Standards Institute. (2008). *Chief security officer (CSO) organizational standard (ASIS CS0.1-2008), American National Standard.* Alexandria, VA: ASIS.

ASIS International and Society for Human Resource Management. (2011). *Workplace violence prevention and intervention (ASIS/SHRM WVPI.1-2011), American National Standard.* Alexandria, VA: ASIS.

ASIS Utilities Security Council. (2012). *Utilities critical infrastructure protection: Security dependencies and trends.* Alexandria, VA: ASIS.

Barton, D., & Court, D. (2012, October). Making advanced analytics work for you, *Harvard Business Review.*

Brown, B., Chui, M., & Manyika, J. (2011, October). Are you ready for the era of 'big data'?, *McKinsey Quarterly.*

Brynjolfsson, E., Hitt, L., & Kim, H. (2011, April). Strength in numbers: How does data-driven decision making affect firm performance?, *Social Science Research Network.*

Campbell, G. (2012). Driving excellence in enterprise security. Report of the Security Executive Council.

Campbell, G. (2012, November). What is excellence. *Security.*

Carnegie Mellon University. (1995). Security metrics. In *Systems Security Engineering - Capability Maturity Model.* http://www.sse-cmm.org/metric/metric.asp

Clark, S. (2013, February). Minimize risk, maximize your protection. *Security.*

CSO Roundtable. (2010). *Enterprise security risk management: How great risks lead to great deeds.* Alexandria, VA: ASIS International.

Hodgkin, K. (2011, July 26). Interview with author.

Hoffman, C. (2012). Presentation within *Data Mining and Statistical Measurement in Retail Loss Prevention*, ASIS International 58th Annual Seminar and Exhibits.

Kiron, D., Shockley, R., Kruschwitz, N., Finch G., & Haydock, M. (2011, Fall). Analytics: The widening divide, *MIT Sloan Management Review Research Report.*

McAfee, A., & Brynjolfsson, E. (2012, October). Big data: The management revolution, *Harvard Business Review.*

McIlravey, B. (2009). Security information management—The foundation of enterprise security. Edmonton, Alberta: PPM 2000 Inc.

McIlravey, B., & Ohlhausen, P. (2012). Metrics and analysis in security management. Edmonton, Alberta: PPM 2000 Inc.

McKinsey & Company. (2012). *McKinsey global survey results: Minding your digital business.* New York, NY: McKinsey.

Slotnick, J. (2012). *The new enterprise security risk manager.* Presentation at ASIS International 58th Annual Seminar and Exhibits.

Tuskan, B. (2011, January 27). Interview with author.

Worman, R. (2012). *The value stream of security.* San Francisco, CA: The Sage Group.

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

1-888-776-9776
1-780-448-0616
information@ppm2000.com
www.ppm2000.com

Microsoft Partner
Gold Independent Software Vendor (ISV)

PPM