ARTICLE COURTESY OF LEXICON SYSTEMS, LLC | +1 281.280.8106 | lexicon-systems.com

Agile Incident Management Systems

Incident management is a strategic issue, no longer the sole domain of environmental, safety, and emergency response personnel. Recent incidents with far-reaching environment, health, and safety (EH&S) consequences have dominated news headlines for months, capturing worldwide attention. Serious incidents can cause loss of life, loss of business, large financial impacts, and damage to the reputation of the companies involved.

by Jill Gilbert

Jill Barson Gilbert, QEP, is president of Lexicon Systems, LLC. E-mail: jbgilbert@lexicon-systems.com.

This column marks the 10th anniversary of *IT Insight*. Congratulations Jill! E-mail em@awma.org and/or jbgilbert@lexicon-systems.com to let us know what you'd like to see discussed in future columns.

On the surface, incident management sounds straightforward—if you prefer a reactive approach—but organizations that take a proactive approach meet certain challenges such as tracking follow-up action items to closure, using management data proactively, sharing best practices and lessons learned, and perhaps most important, predicting future performance.

The Incident Lifecycle

An ***incident*** is an unplanned event, an occurrence, natural or manmade, that requires a response to protect life or property. Incidents can occur anywhere within a business enterprise. They exist in many forms, from releases to the environment, occupational injuries and illnesses, or regulatory compliance variances to customer complaints, information technology, or product quality issues. In IT parlance, an incident is any event that is not part of the standard operation; it results from failure of the infrastructure and has a root cause.[1]

Incident management refers to tracking an incident through its lifecycle, from discovery through corrective and preventive actions, investigation and root cause analysis to closure.

The ***incident lifecycle*** includes several common processes:[2]

- incident detection and reporting;
- classification and initial support;
- investigation and diagnosis;
- resolution and recovery;
- incident closure; and
- incident ownership monitoring, tracking, and communication.

Organizations handle most incidents locally, with little or no outside assistance. In the United States, the National Incident Management System (NIMS) provides a comprehensive, systematic approach for managing complex incidents that require the involvement of a wide cross-section of resources and jurisdictions.[3] This column focuses on information management rather than incident command and control.

Issues and Challenges

The Knowledge Worker Syndrome

A knowledge worker is an individual highly valued for his/her ability to interpret information within a specific subject area, for instance, an EH&S professional, operations manager, or vice president.

Once an incident occurs, a knowledge worker "owns" the incident and has the responsibility to track the incident through its lifecycle to closure. Organizations universally struggle to crack the code for improving the effectiveness of knowledge workers who must make complex decisions based on knowledge and judgment. The stakes are high: raising the productivity of these workers, who constitute a large and growing share of the workforce in developed economies, represents a major opportunity for companies.[4]

Performance metrics are hard to come by in knowledge work, making it challenging to manage improvement efforts (which often lack a clear owner in the first place). Against this backdrop, it's perhaps unsurprising that many companies settle for scattershot investments in training and IT systems.[4]

Productivity barriers that impede half of the interactions of knowledge workers include

- physical (geographic and time zones);
- technical (lack of tools for locating the right people and collaborating);
- social or cultural;

- contextual (struggle to share and translate knowledge obtained from colleagues in different fields); and
- temporal (time, or the perceived lack of it).

Spreadsheets and One-Off Databases

Many EH&S professionals use spreadsheets and "one-off" custom databases to manage incident data. We use spreadsheets because we are comfortable with them; to use anything else requires learning a new system. However, this results in several versions of the truth, inconsistent data, inefficient processes, and requires time to aggregate information. Spreadsheets and one-off databases pose several challenges, including

- following up on action items and tracking through closure;
- using other enterprise data (e.g., physical assets and equipment data when operations incidents trigger "management of change" requirements or human resources data when an occupational injury or illness occurs);
- using management data proactively, predicting future performance; and
- relating incidents to risks.

Spreadsheets and small databases also create challenges with respect to accountability, transparency, and data privacy. Because only a select few can access the information, rather than sharing information with the appropriate parties across the enterprise, these systems limit the ability to track key performance indicators (KPIs).

The Agile Incident Management System

A well-designed, integrated software application can automate the incident management lifecycle, reducing risk across the enterprise. Today, organizations can choose from several integrated commercial EH&S incident management software packages.

Characteristics

Whether commercial software or developed in-house, an agile incident management system should embrace the following characteristics: life cycle management, data integration, collaboration, reporting, and adaptability (see Table 1).

Table 1. Elements of an agile incident management system.

Element	Software Characteristics
Incident lifecycle management	Automated workflows Lifecycle steps (i.e., risk identification, incident tracking, investigation, corrective/preventive actions)
Data interfaces and integration	Audits/assessments/questionnaires Action item/task management Alerts and notifications Asset management Human resources data integration Electronic content management Other systems*
Collaboration	(Web) portal Document routing (see automated workflows) Shared workspaces
Reporting	Internal and external Roll-up reporting Dashboards and scorecards KPIs Transparency
Adaptability	Flexible Ease of configuration and implementation Information security Software-as-a-service* Mobile applications* Offline use*

Notes: *Optional features.

Benefits

Moving to a robust, integrated software application helps increase knowledge worker productivity and operational effectiveness. An agile system helps organizations standardize each critical process throughout the incident management lifecycle. Drawing from shared data on single platform, it promotes collaboration to support better decision making.

An agile software application allows predictive analysis (e.g., analysis of root cause trends). It provides the organization with greater insight into and control of operational risk through a centralized risk database, alerts, and feedback system.

Organizations that adopt integrated incident management software can gain insight into their operations and reduce risk. A well-designed system can provide timely information to the right parties, foster accountability and transparency, and provide data privacy.

Look before you leap… as with any new business system, develop a strategy, understand your incident management objectives, and prioritize your needs before launching into a new software project. em

References

1. ISO 20000:2005. IT Service Management.
2. Borrowed from the IT Infrastructure Library/ISO 20000:2005.
3. U.S. Department of Homeland Security, National Incident Management System Core Document, December 2008.
4. Matson, E.; Prusak, L. Boosting the Productivity of Knowledge Workers; *McKinsey Quarterly*, September 2010.