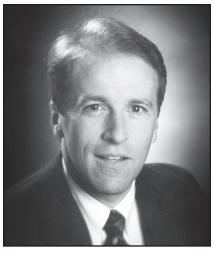
Leverage Complex Event Processing to Improve Operational Performance

Alan Lundberg



Alan Lundberg is senior product marketing manager for TIBCO.
alundber@tibco.com

No one would argue that the state of business today isn't highly complex, particularly where information systems are concerned; and few would argue that complexity adds business value. A closer look, however, reveals that part of the problem arises from data integration challenges and an overabundance of data.

The irony is that advances in technology have made possible immediate access to more and more relevant data. Immediate access to a crushing load of data doesn't automatically translate to business insight, agility, and competitive advantage. In fact, without an effective means of collecting, analyzing, correlating, and applying the data, it can and does have the opposite effect—information overload.

In addition to becoming more complex, the speed at which data is being produced is increasing at the same time as the velocity and speed of business is increasing.

- Documents can be sent in 30 seconds rather than three days
- Stock trades can be settled in less than a day
- Airline tickets can be bought in 20 seconds instead of 20 minutes

At the same time, customer service response-time expectations have shortened dramatically. If you then add data associated with business processes, policies and procedures, workflow, techniques, or strategies and tactics, the combined complexities produce unmanageable amounts of information in many different formats. The current tendency to deploy discrete hardware and

software solutions to address this business challenge may simply add to the problem.

Still, there is hope. The complex interrelations and overabundance of data, if leveraged properly, can provide companies with a vital strategic advantage. In fact, more companies are seeking solutions that allow them to respond in real time and to move toward predictive business, an exciting approach that makes it possible to anticipate customer needs, create opportunities, and avoid potential problems.

Based on the real-time movement of data across the enterprise, the best of these new solutions uniquely correlates information about a company's operations and performance with information about expected behavior and business rules. This capability makes it possible for decision makers to anticipate and respond to threats and capitalize on opportunities before they occur, enabling the next step in the evolution of a real-time enterprise: predictive business.

A New (Old) Approach: Events

Business operations consist of events or micro-events, the everyday millisecond-long occurrences that are the fabric of enterprise activities. A typical business may produce millions of events on a daily basis. These events can be created through employee or customer and vendor relationships, and can include data or messages that record business activity. Traditionally, these events are captured in dedicated applications or run on their own, without significant oversight. If captured, the information they generate is often available from siloed storage that may or may not interoperate with other enterprise solutions.

As organizations increasingly leverage their everyday events through event-driven architecture (EDA) and event-driven business processes, workflows, and applications, they can use new techniques such as complex event processing (CEP) to derive more value from their infrastructure and, ultimately, their operations.

This article examines the ideas and the impact of CEP on businesses, and shows that by developing a comprehensive, interrelated repository of micro-events, businesses can see trends, patterns, potential areas of opportunity, and even areas of potential threat. In short, they can identify trends or scenarios that require immediate attention to increase real-time responsiveness and operational efficiency, an immensely valuable capability. CEP is powerful because its degree of access and visibility allows businesses to anticipate or predict customer needs, make faster decisions, and take decisive action.

Improving Visibility and Agility

Over the past decade, businesses have created complex, heterogeneous IT environments through technology purchases, outsourcing initiatives, and consolidation. While software can help businesses more easily connect key systems and coordinate critical processes, many activities remain unstructured and unpredictable. The nature of these interactions makes it difficult to measure and manage performance proactively.

Today's business environment demands agility. Organizations must be able to manage an unprecedented volume of real-time information about performance, internal operations, and the operations of the value chain. To successfully manage these factors, organizations must be able to observe and understand events across the extended enterprise. They must also consider regulatory requirements, risk management, and the need to respond rapidly to changing market conditions. They must extract high-level business impact from a myriad of business-unit-level processes and seemingly unrelated events across operational layers.

Businesses need a methodology that lets them capture events regardless of where they occur. With CEP, businesses can map events to expected outcomes and relate events to key performance indicators (KPIs) such as their effects on revenue, cost of operations, and business risk. CEP gives businesses insight into the events with the greatest business impact.

Current Challenges

Typically, businesses analyze historical performance trends in an effort to link causes and events. Their prime

concerns are to develop new customer up-sell, cross-sell, acquisition, and retention strategies and prevent recurring problems. If they cannot analyze performance in real time, however, businesses limit their ability to capitalize on opportunities, potentially missing them altogether. The business and IT layers in an organization may often seem disconnected (see Figure 1), especially regarding the causes and effects of an organization's daily events.

Consider two chains of events with the same result—a canceled customer order.

In the first chain of events, a salesperson submits an order through the company's ERP system. Unfortunately, a router is down and the order is not forwarded to fulfillment. The customer calls fulfillment to check the order's status, but fulfillment is not aware of the order. After a few unsuccessful attempts to track the order, the customer cancels it and orders from a competitor.

In the second chain of events, a salesperson submits the order via the company's ERP system. Shipping receives the order, assembles it, plans the delivery route, and loads the order on a truck. Unfortunately, the driver goes to the wrong airport. Re-routed to the correct airport, the driver misses the flight. When the order arrives late, the customer cancels it and orders from a competitor.

In both scenarios, the salesperson must rebuild the relationship with the customer. To avoid these types of situations, businesses have invested heavily in customer relationship management (CRM), business intelligence (BI), and data warehouse (DW) applications. However, these approaches fall short in providing information that a customer is about to defect.

Application-driven approaches are not enterprise-focused; neither do they provide total visibility. CRM applications address the data and workflow surrounding customer contact. BI and DW applications provide historical context. Even when they are integrated, they cannot ensure best possible action or consistency across the value chain. They cannot recommend analysis that ties outcomes to profitability goals.

Newer architectural approaches such as service-oriented architectures (SOA) and electronic design automation (EDA) drive the availability and exchange of an

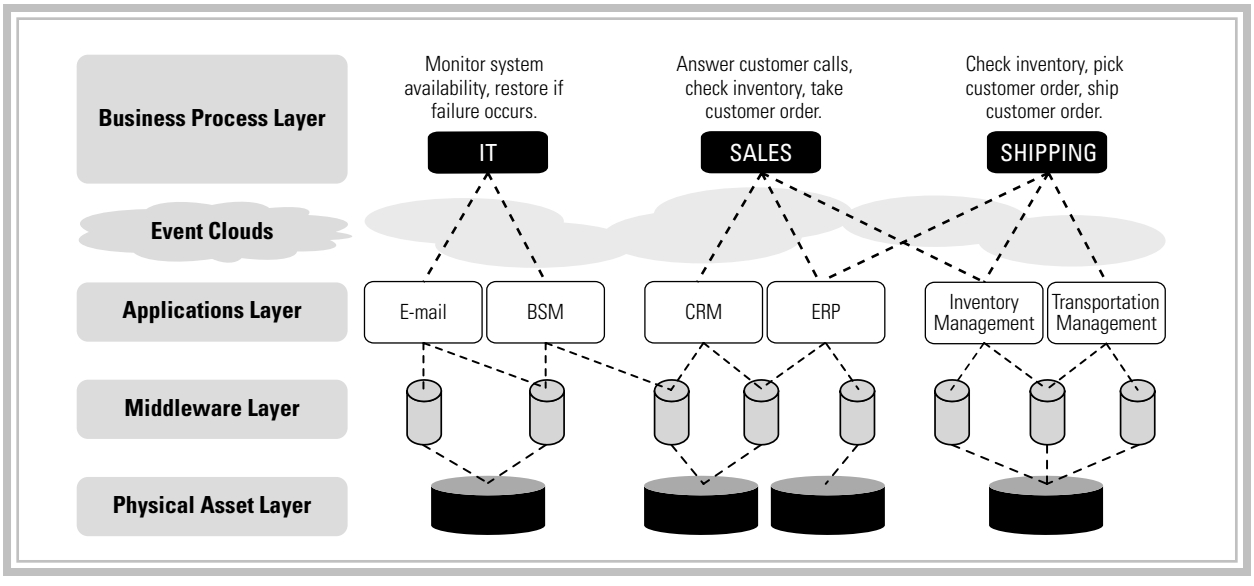


Figure 1. *Enterprise IT Layers. CEP is a new technology for detecting business conditions by monitoring a flow of events and recognizing patterns in higher-level business events as they occur between the IT and business layers in an organization.*

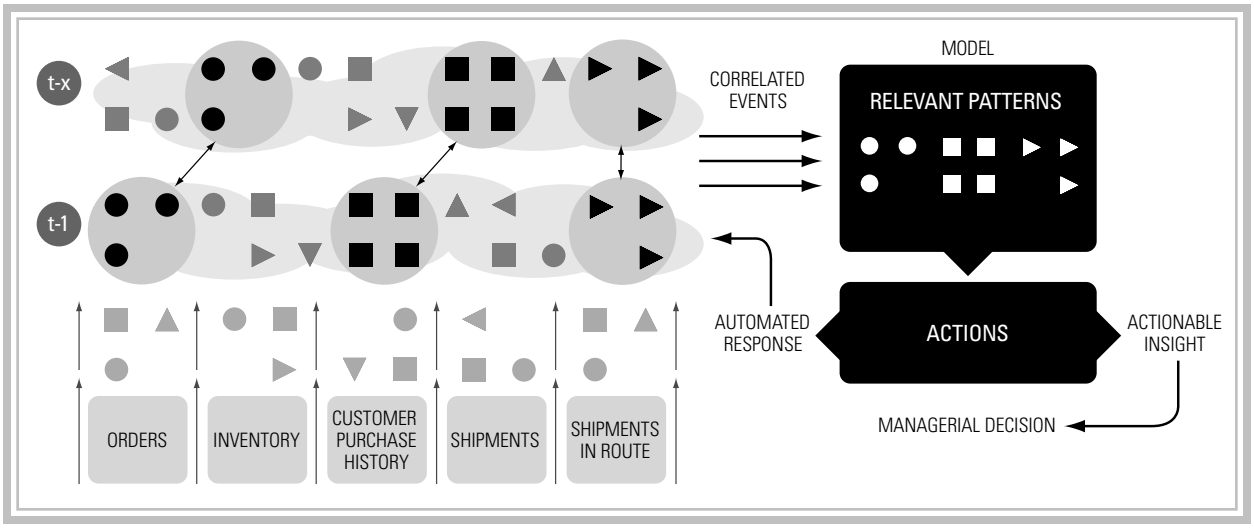


Figure 2. *CEP delivers insight from enterprise events*

unprecedented volume of real-time information about enterprise performance, internal operations, and the operations of the value chain. SOA and EDA may enable businesses to access events in real time and research information about past events, but they still need additional capability to provide business insight—the ability to detect patterns of events in the IT layers of the enterprise and predict how they will impact high-level goals, policies, and processes.

To effectively manage enterprise events, businesses need a real-time architecture that can reveal events and patterns that are critical to survival and present actionable insight that is consistent with KPIs, which is where CEP enters the picture.

Complex Event Processing

CEP is an emerging rule-based technology that aggregates real-time information from distributed message-based systems, databases, and applications. CEP dynamically reveals patterns and trends that would otherwise go unnoticed. CEP allows companies to identify and anticipate opportunities represented by seemingly unrelated events across complex, heterogeneous IT environments. Figure 2 shows how CEP extracts these insights.

Today, businesses capture hundreds of thousands of business events to form what Stanford University's David Luckham (see sidebar, page 60) refers to as an event cloud. These events can include updates to customer records in a CRM application, sales in a point-of-sale application, orders scanned upon shipping or delivery, GPS data for delivery trucks, weather information, and RFID data for pallets or display stands.

Key to CEP implementation is the ability to model business operations, specifically the dependencies among servers, network infrastructure, applications, people, and processes. CEP uses these models to identify constraints or patterns that map formal or informal processes to expected outcomes. These models provide a framework for designing, automating, and managing intelligent decisions across the enterprise.

With models created, CEP compares previous or expected values to real-time events, accounting for timing relationships and reducing the number of events managers must react to. Business rules relate activities to the processes they support, and enable enterprises to develop pattern-triggered actions, freeing managers to handle unexpected or unstructured events.

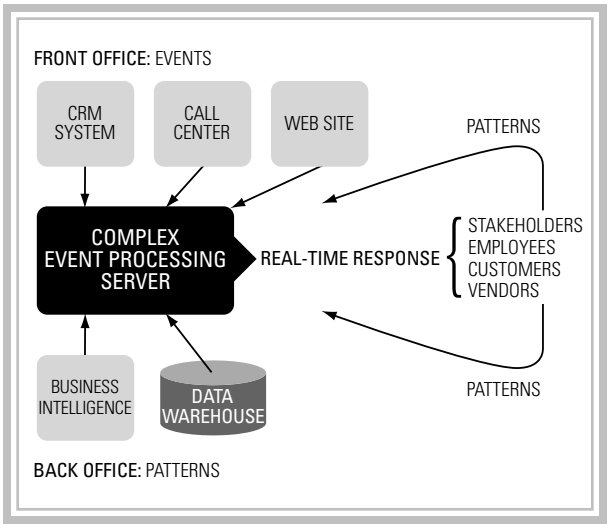


Figure 3. *CEP Systems are noted for their ability to provide insight into operations in real time. They are iterative and can create new events as patterns of activity from employees, vendors, customers, and other stakeholders emerge.*

To illustrate how CEP works, consider the canceled customer order examples mentioned previously. In the first scenario, if you knew a router was not working (or was about to fail) and you knew precisely the potential effects on timely delivery, accounts payable, and (most important) customer service, you might have enough time to fix the router, or reroute delivery to avoid any delay in delivery to fulfillment.

In the second scenario, if you are alerted of the driver error in real time, you can inform the customer of the delay and proactively offer discount coupons on future orders. By preemptively taking action to solve the outage issue and demonstrate your appreciation for your client, your organization stands a good chance of avoiding potential revenue loss from the outage and retaining the customer.

Implementing CEP

Implementing CEP in today's IT environments is an engaging challenge. The increased corporate complexity makes it difficult to measure and manage operational performance, causing businesses to react to inaccurate or conflicting data instead of proactively managing their operations. Adding additional software can be overwhelming and futile. CEP systems might be worth the effort, however, if the application creates the organizational ability to detect situations that need immediate attention, such as threats or opportunities.

There are many types of CEP systems and approaches to implementation. These steps are commonly taken to implement a CEP application:

1. Instrument the enterprise to capture events.
2. Correlate/match these events to business objects for context and to determine causality.
3. Create the capability to recognize event patterns.
4. Once patterns are recognized, aggregate pertinent event patterns into higher-level event structures also known as "complex" events.
5. Provide business process models and state-based timing expectations (e.g., timeouts/lack of event support) to represent meaningful process transitions.
6. Create the capability to (re)act to drive the business object state to mitigate problems or take advantage of opportunities.

These steps form the building blocks of a CEP system: you must identify your business events, enable your system to recognize the events, and create relevant or meaningful patterns. Meaningful patterns might be reactive (as in root cause) or predictive (as in early warning patterns). Once the CEP system is set up to identify the patterns, you can apply business rules and models that will help operations automatically act towards the pre-defined goal.

When possible, involve business users in determining business rules and process flow to ensure efficacy, and utilize industry standards such as UML, XSD, XSLT, and WSDL to ensure interoperability.

Among the standard software components in a CEP system:

- Channels for connecting an enterprise-level, multi-channel service bus (ESB) that facilitates the integration of various legacy systems while providing a standard, universally-accessible distributed service protocol

- A "state" monitoring function that follows the state of an event as it evolves with time (changes or transitions its state)
- Dependency correlation document that maps asset and process dependencies and causalities
- A business rules engine that is connected to an environment that allows rules to be applied to real business events that occur throughout the enterprise

Channels
Channels are one of the delivery methods for transporting a company's events. Events are captured into a CEP system via external messaging channels, or they can be generated from inside the engine via previously-referenced rule action. Events can contain data in properties and payload. Properties are data elements belonging to an event that are accessible to the rules engine. Payload is inaccessible data contained within the event, being transported by the event. When used in combination with a state machine, a captured event will remain in the event processing engine until it is expired by time or explicitly consumed by the rule engine.

State Machine
The state model, or state machine, is a perspective of the object model in which objects are viewed as having defined states and the transitions from one to another are viewed as separate objects.

For instance, consider the earlier example of a product order as it follows its life cycle. The order is received, then assembled, shipped, and invoiced. All these states should be represented as objects in a state model. Each state can be managed independently and is important in track-and-trace or quality-control applications.

Rules/Inference: Automatic Execution of Dependent Rules
At the core of a CEP system is a declarative business rules engine that receives and correlates events and applies rules as needed. The rules engine can then generate internal events, which could trigger more rules or send events out.

The declarative nature of most rule-based systems means that rules are evaluated if the fact (property/relationship of an object) it is referencing is created or changed—an important consideration in a large-scale deployment. In other words, it only evaluates new input, not the whole rule network, every time something changes. This allows the rules to be designed independently of each other (rules are standalone pieces of knowledge; they don't know about each other).

Sample:
Rule 1:
If cust.airmiles>1000000 then cust.status="platinum"

Rule 2:
If cust.status="platinum"
then cust.miles_credit_limit=500000

Rule 3:
If cust.miles_credit>cust.miles_credit_limit
then createevent(credit_limit_exceeded)

Complex Event Processing Theory

Complex event processing, developed by David Luckham of Stanford University, extends the Holland Complex Adaptive Systems model developed by John Holland in 1976 to model how organizations use knowledge to adapt to their environments.

Part of this theory states that an organization is a complex system with the ability to change its rules as experience accumulates. The key is to identify action rules based on IF/THEN statements. That is, IF certain conditions occur, THEN certain adjustments can be made.

In attempting to adapt to changing circumstances, an organization develops rules or models that anticipate the consequences of responses. At its simplest level, this process is not significantly different from Pavlovian conditioning. Building on Holland's work, Luckham started to apply the concept of using business events to solve business problems.

In these rules:

- Forward inferencing (forward chaining) means that Rule 2 fires automatically if Rule 1 changes the status of a customer to platinum, because one of the facts referenced by Rule 2 has changed.
- Rule 2 will not be fired if the customer status has already been "platinum" before, only if it has changed.

Rules can also be grouped logically; at run time you determine which rule groups are active or partition them to separate event-server engines. Rule functions can be defined for re-use throughout the CEP project.

The goal is to leverage existing infrastructure and existing assets—you are essentially setting up your system to be extracting as much event data as possible from your current operations to eventually be able to detect patterns, predict threats, or identify potential opportunities.

Some companies believe this can be accomplished with databases. While possible, it's difficult. With databases, you must contend with static relationships, rigid schemas, and siloed event clouds, as opposed to enterprise event clouds with CEP. There is also a lack of visibility into temporal relationships, which are important to track in dynamic and complex business processes. Remember, complexity or information overload is an accepted reality in most operations, as are the indiscernible early warning patterns. CEP is a new tool for operations to leverage existing infrastructure to detect and process this information.

The interesting footnote to this technology is that many of the ideas comprising CEP are based on artificial intelligence (AI) or expert systems of many years ago. It might seem unwise to mention this CEP association with AI and its infamous hype and unfulfilled potential, but AI's foundational capabilities have been quietly subsumed into many common and accepted systems and applications. Business-rule processing firmly addresses numerous problem areas of today's IT organization. With CEP, though, it's the addition of all the previously missing elements in an enterprise system with ubiquitous real-time data feeds that has enabled the timeliness of this whole new class of application that can, in turn, address a new set of business/IT problems.

Some industry analysts have described CEP systems as a next-generation framework for event-driven, reactive systems such as dynamic pricing, utility computing, monitoring, and management. Consider some of the other areas where CEP can be applied:

- A technician is dispatched to a customer location. While in transit, the customer cancels the order. In the same time frame, another customer in the vicinity places an order. The technician is dynamically re-routed to the new customer.
- A brokerage detects unusual call-option activity from a customer who has rarely traded in options or futures. This unusual activity triggers trading limits based on velocity and magnitude of trades for the brokerage to manage risk and alerts customer service so they can proactively contact the customer and verify the transaction.
- A pallet of pharmaceuticals in transit within the logistics supply chain needs to be recalled for quality control purposes. Radio frequency identification (RFID) location and pallet identification events are tracked and the pallet is intercepted prior to breakdown and retail distribution.
- An independent power operator notices peak load changes across the power grid with the potential to disrupt service to large portions of the community. These operational, real-time events are understood to fall into a pattern that is recoverable based on dynamic allocation and load management across the grid. No subsequent outage is experienced.

How CEP Can Solve Real Problems

We offer several examples to show the practical nature of CEP.

Service Assurance

With commoditized products and ever-shortening product life cycles, companies seek to distinguish themselves

CEP in Banking

A major bank is attempting to reduce its exposure to fraudulent activities such as money laundering and credit-identity theft.

The bank has seen significant losses from successful online "phishing" expeditions aimed at its online banking and credit card customers. Phishing is an online scam where criminals pose as banks and other legitimate businesses soliciting customer passwords, bank account numbers, and other sensitive information via e-mail.

In a recent report, the Gartner Group warns that phishing threatens the viability of e-commerce and online financial activity, and estimates it cost U.S. credit card companies and banks more than $1.2 billion in 2004. (Gartner, 2004) This bank's challenge is to stop or minimize the effects of phishing expeditions. To do so requires a solution that recognizes a pattern of fraudulent behavior and correlates it across different silos such as ATM activity, mortgage and credit card applications, and online banking. Because fraud is typically a multi-pronged effort, the ability to perform real-time correlations can significantly mitigate its effects.

A CEP solution can detect many of the micro-events that comprise a bank's business. These events range from online access to trades to phone calls regarding account reconciliation, and even to virtual events, which are supposed to take place (but may not), such as periodic timed, wire-currency transfers. The system can detect anomalies in online banking, new account set-up, changes in passwords or beneficiaries, or even server-image downloads that might indicate phishers are trying to redirect traffic to their server. Once detected and aggregated, the system can use rules to prevent online transactions or new credit card applications from being processed. It could assign new account numbers and/or notify customers or authorities if the perpetrators can be identified. It can also sense and respond with new security event rules as hackers change their tactics.

by offering a higher quality of service (QOS) at a lower cost. Those best able to control their assets, including network, service infrastructure, customers, and supply chain partners, have a competitive advantage.

Organizations have leveraged BPM applications to deliver value cost-effectively. These solutions improve efficiency within divisions, reducing, for example, the time needed to process an individual order. However, they provide less insight into the impact of missing a scheduled delivery to a high-value customer. To build the infrastructure required to create, deliver, and support new products and services consistently, companies must supplement BPM with CEP solutions. The real-time process integration and management infrastructure provided by CEP incorporates service events and metrics at the most granular level, allowing businesses to capture customer incident metrics and understand the impact on customer satisfaction, service level agreements (SLAs), and the bottom line.

CEP-based service assurance solutions can aid in:

- End-to-end process visibility and insight, regardless of the business domain
- Role-based visualization and real-time analytics around service assurance
- Service event/metrics interpretation and correlation, including business impact and insight into KPIs
- Trending and real-time performance forecasting
- Auditable reporting as well as event- and scenario- persistence capabilities
- Real-time awareness into the potential for customer defection

There are three significant benefits from a CEP solution:

- **Reduced operating costs:** End-to-end performance monitoring, visibility, and alerts enable organizations to rapidly identify potential SLA violations, restore the network rapidly, or resume normal operations at the customer site
- **Enhanced productivity:** Insight into operations through metrics that tie assets and events to quantifiable business impact lets companies fine-tune business processes; the correlation between SLA performance and industry metrics such as Six Sigma provides tangible QOS improvement.
- **Lower risk of customer defection:** The ability to view enterprise events in the context of KPIs allows companies to proactively identify and manage risk of non-compliance, focusing on customers with the greatest effect on the business

Program Trading: A Pot ent CEP Example
According to the New York Stock Exchange, approximately 50 percent of its weekly trades are program trades, the simultaneous trading of a portfolio of 15 or more stocks with an aggregate value in excess of $1 million. Financial institutions increasingly seek to execute program trades to capitalize on shifts inside sectors, shifts between sectors, pair trading strategies, portfolio rebalancing, and other multiple stock/order strategies. With the regulation to modernize the National Market System [Reg NMS], the NYSE hybrid market, and new trading volume records seemingly set every month, electronic and program trading volumes will continue to increase.

CEP-based program trading solutions provide a high performance, agent-based architecture that collects financial data and correlates it according to specific rules and patterns that identify potential arbitrage and market opportunities in real time. With these solutions, financial services companies have the advantages of:

- Scalable infrastructure for managing large volumes of real-time events
- Complex sequencing with finite-state, machine-based reasoning
- Trending and real-time performance forecasting
- The ability to quickly deploy trading models across the organization
- Auditable reporting and event persistence capabilities

Using CEP to Enable Predictive Business
The ability to incorporate real-time information and complex event patterns into business decisions is critical to an organization's success in fast moving marketplaces, but it is only the beginning. Once in place, CEP solutions, in combination with relevant historical information derived from analytics software, can be used to enable the next phase of the real-time business, the *predictive business*.

Predictive business builds on the capabilities of real-time business to address these requirements. To enable predictive business, enterprises must put the following infrastructure in place:

- Organizations must be able to establish business-process definitions and support the IT infrastructure so process definitions are automatically adapted on the fly as business scenarios occur, new factors are revealed, and business activities are completed.
- The IT infrastructure must be able to capture and correlate large numbers of events so it can automatically recognize and identify potential problems and opportunities. Appropriate IT and business people must be notified instantly about situations that require their attention, giving them the opportunity to initiate a course of action with the highest probability of delivering maximum value.

The goal of real-time business is to enable an enterprise to recognize situations as soon as possible and solve the problem or take advantage of the opportunity. Many business operations, however, follow patterns that, if identified, would allow companies to address problems or opportunities literally as they arise. As more companies

achieve the operational advantages of real-time business, leaders need to take the next step to distinguish themselves and sustain their competitive advantage.

Real-time business is about doing things faster. Predictive business is about doing things that were impossible before. For example:

- In real-time business, the goal is to respond to problems faster than one's competitors. In predictive business, the goal is to avoid problems altogether.
- Where real-time business allows companies to move swiftly to resolve a customer need, predictive business helps an organization anticipate the need and provide the opportunity to address the need before the customer takes action.
- Where a real-time business can move quickly to capitalize on an opportunity before its competitors act, predictive business helps a company create new ways to serve existing c ustomers or open new markets.

Predictive business builds on real-time business' core values: identify a situation, make a quick decision, and take action. The difference is that a problem or opportunity can be identified before the event that creates the problem or opportunity occurs. The implications for future business are immense. Predictive business can help organizations improve their ability to service customers and drive revenue in many ways:

- Orders from a major customer are trending down during peak season. Is there a danger of losing the customer? Predictive business can help identify patterns such as decreasing orders from a major customer during a typically busy period. This might trigger an investigation or a program to stimulate buying behavior. This problem typically would not be noticed, nor could it be addressed, without CEP technology.
- Based on trends, a customer will need more bandwidth in one week. Where is the optimal point to begin up-selling? In this scenario, predictive business helps anticipate increased demand before the customer calls with the request. Based on similar customer usage, trending information, and real-time data, the system can recommend (and provide a telemarketing script with) customer specifics designed to support up-selling.
- The current trend is toward SLA thresholds. How can resources be reallocated to ensure continued compliance? In this scenario, risk management techniques compare fixed support costs with costs of SLA penalties to determine how a violation may affect the business and identify the best course of action.

Conclusion

Once a requirement for large, IT-centric organizations, real-time and predictive business architectures built on CEP are becoming a priority for organizations of all sizes. As the pace of business accelerates and increasing regulation and global competition drive tighter control over operations, midsize and large companies must find cost-effective ways to increase their agility and customer retention. They can no longer afford to extend packaged legacy and custom applications that perform specific business functions or simply analyze historical corporate performance trends. This data becomes stale if it is not used to anticipate events before they happen.

Businesses need a methodology to capture granular, real-time events from multiple sources at different organizational layers across the value chain. They must commit to deploying solutions that put the volume and variety of data they deal with daily to optimal use. In such a competitive environment, seemingly small errors can easily turn a customer to another organization that promises superior service or enticing benefits. By leveraging existing data, companies can anticipate these errors, predict the reactions, and act on potential problems or issues caused by an error even before the error occurs.

Through CEP-based solutions, businesses have a "model to code" approach for building event-driven applications

that provide enterprise visibility and information triggers. Integrating CEP into a highly responsive, real-time enterprise architecture allows companies to identify and anticipate exceptions and opportunities represented by seemingly unrelated events across complex, distributed, heterogeneous IT environments. With CEP, organizations acquire the wider insight into events that allows them to identify those that have (or will have) the greatest business impact, enabling them to improve operational performance. ■

REFERENCE

Litan, Avivah (Gartner Group). "Phishing Victims Likely Will Suffer Identity Theft Fraud," May 14, 2004.

Instructions for Authors

Editorial Acceptance

- All articles are reviewed by the *Journal's* editors before they are accepted for publication.
- The Publisher will copy edit the final manuscript for conformance to its standards of grammar, style, format, and length.
- Articles must not have been published previously without the knowledge of the Publisher. Submission of a manuscript implies the authors' assurance that the same work has not been, will not be, and is not presently submitted elsewhere.
- Authors will be required to sign a release form before the article is published; this agreement is available on request (mmcfarland@tdwi.org).
- The *Journal* will not publish articles that market, advertise, or promote one particular product or company.

Submission of Materials

Materials should be submitted to:

Marie McFarland
Business Intelligence Journal
TDWI
5200 Southcenter Boulevard, Suite 250
Seattle, WA 98188
206-246-5059, ext. 110
Fax: 206-246-5952
E-mail: mmcfarland@tdwi.org

Visit http://www.tdwi.org/journal.htm for a complete list of the *Business Intelligence Journal's* submissions guidelines, including writing requirements and editorial topics.

For *Journal* advertising rates and information, please contact Steve Cissell at 206.246.5059, ext. 114, or scissell@tdwi.org

Upcoming Submission Deadlines

V11N2
Distribution: June 23, 2006

V11N3
Submissions Deadline: June 2, 2006
Distribution: September 8, 2006

V11N4
Submissions Deadline: August 18, 2006
Distribution: December 15, 2006