June 14, 2010

Case Study: AMERICAN SYSTEMS Demonstrates The Value Of Business Service Management

From Reactive To Proactive: Using Service Management To Leverage Integrated Event Correlation

by Evelyn Hubbert
with Robert Whiteley and Ben Echols

EXECUTIVE SUMMARY

The IT and business alignment discussion is not new: Many IT organizations have been trying to become aligned with their business units or overall business goals. Understanding what it means to be aligned and then actually implementing alignment is at the heart of an IT management strategy called business service management (BSM). This strategy (or approach or methodology) aligns IT elements such as applications and infrastructure components and processes in a way that supports the goals of the business. AMERICAN SYSTEMS wanted to improve the delivery and quality of its services to the business. The company introduced ITIL and COBIT standards and deployed integrated data center management software to gain situational awareness, preempt and respond to issues more efficiently, and better protect information assets.

SITUATION: AMERICAN SYSTEMS NEEDED TO MOVE OUT OF A SILOED APPROACH

Many IT operations teams find themselves managing in application-centric or domain-centric silos. This mentality involves technology silos and organizational autonomy and is based on the resources required to manage a particular technology or application. The IT organization at AMERICAN SYSTEMS was trying to manage a variety of pieces — the network, servers, applications — with a variety of management tools. All of these pieces are sources of events that indicate when there is a problem at a particular technology domain. The problem with this approach is that each team had its own event, and it was very difficult to correlate these events to actually understand what needed to be done and where to resolve the root cause and therefore mitigate the impact on the business.

AMERICAN SYSTEMS is a government IT innovator. With the demand for new and better services, the IT organization recognized that it needed to shift away from a reactive and toward a proactive way of managing and operating:

- **AMERICAN SYSTEMS relied on a basic event correlation management approach.** The IT organization had implemented a variety of IT management solutions, but none of them assisted in the coordination of infrastructure- or service-oriented management. It had many disparate systems and data glut (messaging, alerts, and logs) to manage and react to. The IT organization realized that it needed a centralized and more holistic event correlation approach.

- **AMERICAN SYSTEMS' IT organization could not be proactive.** Determining the root cause of a problem and resolving it was too slow and siloed, and the process was very labor intensive — reactive data mining. To become proactive, the IT organization needed to enhance infrastructure monitoring and business service instrumentation, which would allow it to quickly obtain all the pertinent details, collaborate, and see which business services were affected by leveraging cross-system and cross-platform correlation.

- **AMERICAN SYSTEMS' IT management team needed visibility into business health.** Decision-making was based on a variety of teams, inputs, and tools and was therefore difficult and slow. If AMERICAN SYSTEMS could implement more automated dashboards and reports, it could better focus on key issues affecting critical business services, and the decision-making process for changes, incidents, and resources would improve tremendously.

- **AMERICAN SYSTEMS needed to advance security management.** AMERICAN SYSTEMS had installed, enhanced, and upgraded numerous security systems. While this significantly improved the company's overall security posture, it also required more training, coordination, and management. AMERICAN SYSTEMS wanted to advance its security information event management capacity and have more sophisticated methods for performance analysis.

- **AMERICAN SYSTEMS needed to cross-train and transfer knowledge.** The continuous effort of focusing on applications and resolving issues was a drain on resources and inefficient. By cross-training (i.e., blending network engineering and security) and focusing on the delivery of key business services, the IT organization would become agile and able to respond to key problems and changes to improve service reliability, and had more optimized use of its personnel.

BEST PRACTICE: AMERICAN SYSTEMS ADVANCES SERVICES MANAGEMENT

AMERICAN SYSTEMS had defined a variety of goals for its IT organization, which included:

- **Improve security information management capabilities.** The company wanted to enhance security information management capabilities to get ahead of threats and be more responsive and proactive.

- **Centralize security event correlation capabilities.** Many existing tools required different specialized skills to support them, and management and monitoring capabilities were all relatively isolated from each other and did not provide a cohesive and correlated view to support the security team.

- **Adopt best practice processes.** The IT organization needed to implement a variety of best practice processes spanning the different support and delivery deals; the group adopted ITIL, PMBOK, and COBIT, to support the move to a service-oriented group.

- **Implement business service instrumentation.** The IT organization needed to understand the impact on the business services based on an issue or event identified in the managed environment. For this it needed to identify the business services, understand their relationships, and manage these business services from a top-down approach.

Success Came With A Team Lead Approach . . .

A team lead was identified that had the responsibility to take the network operations and security team requirements and determine an approach that would advance general security management and overall network event correlation/management. The initiative relied heavily on selecting a more centralized, flexible, and integrated event correlation system that would integrate within their infrastructure, would manage a significant amount of data, and had analytics that could easily support custom rules and reports.

. . . Coupled With A Data Center Management Solution Provider

The team selected AccelOps as its data center management solution provider, based on meeting the above criteria with an integrated ability to monitor performance metrics, service availability, application response, changes, and security across network devices, systems, applications, storage, virtual environments, and identity. The IT organization already had a good understanding of its business services, because of its supporting applications and infrastructure components, and began to instrument these services with event correlation, service-mapping, reporting, and dashboards. The solution provided the IT organization with the "single pane of glass" to monitor, prioritize, and respond to operational and security issues and support the decision-making process.

A Fool With A Tool Is Still A Fool

AMERICAN SYSTEMS shows how adopting best practices and a business service management approach across its portfolio of applications and IT services can maximize IT resources and contribution to overall business value. But the AMERICAN SYSTEMS experience also demonstrates that technology alone cannot drive big gains in efficiency, function, and service delivery. Rather, AMERICAN SYSTEMS' adoption of a new service management framework that values key processes, overall visibility of impact to key business services, and knowledge transfer allowed them to better purpose resources, be more responsive, and address problems impacting the business. AMERICAN SYSTEMS founded this new strategy on two elements:

- **Implementation of ITIL and other supporting best practices.** The IT organization introduced ITIL best practices for a variety of processes, such as incident, problem, change, and configuration management. It also developed a new management framework aligned with

and based on the company's service offerings. These service offerings were supported with the standard best practice processes. This allowed the IT organization to create an overall service management and governance framework for how it supported the company's overall service offerings. A platform for event correlation would provide the means to monitor and measure IT services, validate change and business impact, as well as adjust resources as needs evolve.

- **Implementation of an event cross-correlation tool.** AMERICAN SYSTEMS took the AccelOps data center management solution, which provided a single console to get insight into many different aspects of the network, the devices that support it, and the related performance and security of those devices — as well as an understanding of the dependencies to support an IT business service.

BEST PRACTICE: AMERICAN SYSTEMS ADVANCES BUSINESS SERVICES AND SECURITY

Instead of a siloed approach to managing applications and infrastructure, AMERICAN SYSTEMS is now managing business services by logically grouping related applications and infrastructure components — monitoring end-to-end in an automated way that correlates performance, availability metrics, and security:

- **A BSM management approach to measure effectiveness.** One of the innovations was to instrument the business services in such a way that they could introduce better metrics measuring the IT organization's effectiveness. Two key metrics introduced were: 1) time to identify, track, and resolve incidents at the business service level, and 2) timeliness of resolution at the business-service level.

- **Effective use of resources.** Because performance metrics and events are now cross-correlated in an automatic way, it reduces the amount of manual analysis and respective resources associated with maintaining IT services. In addition, since the AccelOps platform centrally aggregates and manages the operational data, the IT organization can automate and consolidate reporting (services, performance, security, compliance) and investigation processes rather than relying on numerous tools and dispersed data.

- **End-to-end event correlation that eliminates false positives.** With a management solution (AccelOps) that correlates events across the business services looking at the underlying physical or virtual components, the IT organization can pinpoint a complex problem and understand the root cause faster while eliminating a large number of false positives, which in the past caused a tremendous burden on the IT staff.

- **Converging network and security operations.** By selecting AccelOps, AMERICAN SYSTEMS advanced its security information management capacity to protect its infrastructure and digital assets. AMERICAN SYSTEMS can bring in data from the different security systems, filter

out extraneous noise, respond to sophisticated threats, and enforce custom policies. This also addresses internal security monitoring and compliance.

- **Investment in end-to-end management solution.** AMERICAN SYSTEMS implemented AccelOps as a data center management solution to provide oversight that included comprehensive security information management and the means to monitor and respond to performance, availability, security, and change metrics at both the operations and business service level.

BEST PRACTICE RESULTS: AMERICAN SYSTEMS SHIFTS CULTURE

AMERICAN SYSTEMS' culture changed from an application-siloed, reactive environment to a service-oriented, proactive environment. This benefited both:

- **The team.** The team is provided instant intelligence on its business posture, security threats, and operational performance.
- **The business.** The business is provided a higher level of confidence that the systems are available and performing well and that the networks and data are secure.

RECOMMENDATIONS

A NEW MANAGEMENT FRAMEWORK CAN SHIFT IT FROM REACTIVE TO PROACTIVE

Shifting IT from managing technology silos to managing business services offers significant potential. The primary factor is the ability to see the impact on business services by implementing a top-down approach that helps clarify which are the key business services and which applications and infrastructure components support these business services. Additionally, introducing IT service management frameworks such as ITIL introduces a standard way of doing business and therefore allows IT to apply automation tools to reduce manual efforts from the IT staff.