



IT SOLUTIONS 2006

Progressive Ideas and Leading Technologies

To read full reports and related information, go to the links listed below or visit www.technology-reports.com

Achieving the Promise: IT as Strategic Business Partner

Spurred by new compliance regulations, the rise of outsourcing, flattened budgets, and calls by management to “run IT more like a business,” CIOs are striving to impose formal processes on IT activities. This push for rigor has led many CIOs to begin organizing, managing, and delivering IT in the form of well-defined, tightly-controlled IT services. This is largely uncharted territory for most companies, so it's no surprise that IT organizations are looking for guidance and direction.

IT Service Management (ITSM), as defined by best practices such as the IT Infrastructure Library (ITIL), is often referred to as ERP for IT.

What it represents is a chance for IT to get out from the backbreaking grind of constant firefighting by way of planning, communication, and structured response. Talking to those who have implemented IT Service Management, it is difficult to overstate the potential benefits: reduced costs; improved productivity, communication, and morale; reduced time-to-market; and competitive advantage.

What is often overlooked in the scramble to adopt ITSM/ITIL, however, is that for ITIL to provide the promised returns, it must be applied in a way that leverages specific strengths and mini-

mizes specific weaknesses. Standards are, after all, standard. Companies that do not exercise discipline and restraint in applying ITIL to their specific environment will undoubtedly find themselves faced with yet another revolutionary approach that falls short of expectations.

And yet, it is worth mentioning here that the single biggest reason most IT projects fail has nothing to do with technology, but rather with a lack of participation and buy-in. Change is uncomfortable and must be lead from the top. End users – e.g., lines of business, functional departments, customers, suppliers, and partners – must provide a clear understanding of their requirements and constraints, and be actively involved in discussions of potential benefits and trade-offs.

To read the full report, go to www.technology-reports.com/pepperweed.asp



Pepperweed is one of the largest IT Management practices in the U.S. with over 1200 field implementations. The company has extensive experience in both IT infrastructure and process optimization. All consultants are senior professionals – full-time employees with extensive hands-on field experience. Pepperweed is nationally recognized as a leader in IT Service Management and ITIL, and was recently recognized as an Inc. 500 fastest growing privately held company. **877.984.7575 • www.pepperweed.com**

Data Control and Audit Technology Protects Global Supply Chain Information

As corporations seek to extend their use of offshore suppliers to take advantage of unique expertise, or to reduce the cost of operations, they often expose themselves to increased risk. Sharing intellectual property, financial data, and/or customer private records with offshore partners can often open the door to significant financial loss, or risk to reputation, if the data is misused or compromised. The only hope of maintaining control of these key assets is to protect the data by technical means, or to isolate those who have access to it.

Recent developments in Data Control and Audit technology now make it possible to pro-

tect information where it is most vulnerable – in the hands of end-users as they work with and move data across applications (i.e., office, and remote legacy and Web applications), removable storage devices (i.e., USB flash drives), and various channels of communication (e-mail, Web-mail, FTP, etc.). Data Control and Audit technology automatically monitors the use of data on desktops, laptops, and/or servers, restricting a user's ability to transfer, copy, or print sensitive data based on centrally distributed rules and policies.

This technology has now matured to the

point where it can operate autonomously on a computer device, even when removed from the network. This provides a unique ability to protect multiple types of data, and the integrity of underlying business processes, even in isolated locations within a complex collaborative supply chain. It also has the added effect of creating a “virtual data perimeter” around valuable corporate information and improving accountability, without impacting existing business processes. By using Data Control and Audit technology, it is now possible to centrally protect and track the ‘flow’ of data through a global supply chain, while maintaining a complete audit trail of its use.

To read the full report, go to www.technology-reports.com/Verdasys.asp



Verdasys is a provider of Global Data Security Solutions, protecting data at the “point of use” (on desktops, laptops, and/or servers). We help our customers secure the private and proprietary data essential to running their businesses, data they must entrust to their employees, suppliers, and providers of outsourced services. Verdasys, Inc. • 950 Winter Street • Waltham, MA 02451 • Tel. 781-788-8180 • www.verdasys.com

IT SOLUTIONS 2006
 For in-depth reports on these
 and other technology topics, visit
www.technology-reports.com



To read full reports and related information, go to the links listed below or visit www.technology-reports.com

When 177 Equals 10,000,000,000 (Solving the “Test Coverage” Dilemma)

Technology professionals are daily faced with the decision of how much testing their product needs before it makes it into consumers hands. In fact, time-to-market and cost pressures are just two variables that lead many to the decision to limit or forego testing entirely. An emerging method of test design can provide equal test coverage with 177 test cases vs. 10,000,000,000. To test all combinations of 10 variables with ten values each would require 10,000,000,000 test cases. However, by applying the Combinatorial Method the same test coverage requires only 177 cases.

Using the Combinatorial Method, you design tests that pair each value of each of the variables with each value of each other variable at least once. In Combinatorial Method test design, we are concerned with variables of a system, and the possible values each variable could take. We will generate test cases by pairing values of different variables.

A good starting point for a discussion about Combinatorial Method test design is with Cartesian Products. A Cartesian product is a scenario in which every unit of a group is matched with every unit of every other group,

so that all combinations of units are achieved across all groups.

Consider the following example with 4 variable types: Variable(A) contains integer values 0 through 9, Variable(B) contains all integers 1–99, Variables(C & D) each contains an On/Off checkbox.

How would you test this program? How many combinations are there? There are $10 \times 99 \times 2 \times 2$ or 3,960 possible valid input combinations. The Combinatorial Method of test case design allows companies to achieve an equivalent level of test coverage with only 24 test cases. Equivalent test coverage, improved time-to-market and significant cost savings (win/win/win).

To read the full report, go to
www.technology-reports.com/logikos.asp



Specializing in systems & software design, development & test services. Adept in both real-time embedded platforms and Microsoft Windows®. They assist clients in the following industries: Automotive, Medical Devices, Defense and Consumer Electronics. Expertise with products such as; navigation systems, mobile media, telematics, audio-systems, body electronics, power-train controls, instrumentation & displays, mobile medical devices, wireless-communications, battlefield situational awareness and more... Check them out at: www.logikos.com or send your inquiries to sales@logikos.com.

Accelerate IT with Managed Services

When it comes to deploying and managing IT infrastructure for new applications, a directive often heard from senior management is – “get it done”, usually accompanied by “now”, “make sure it keeps up and running” and, of course, “stay on budget”. For organizations with maxed-out IT staffs and flat-line budgets, it can be a challenge to get these environments up and running quickly. The problem becomes more difficult when 24x7 coverage is needed for support and problem resolution.

Many organizations are turning to Managed Service Providers (MSPs) as an alternative or adjunct to internal IT staff to deploy and operate IT systems. Managed

Services helps companies save money, deploy systems faster and maintain higher levels of service availability and performance. Managed Services allow an organization to focus on what they do best – serve their end-user customers and grow their business – while the MSP does what they do best – manage and support IT systems around the clock with a full team of experts.

Managed Services fall into two general categories: Remote Managed Services and Managed Hosting Services. With Remote Managed services, the MSP monitors and manages the customer’s infrastructure in the customer’s data center. With Managed Hosting Services, the MSP delivers a service to the customer

using the MSP’s hardware and software hosted in the MSP’s secure data center. Hosted Services are ideal for deploying both primary and Disaster Recovery (DR) environments. Some MSPs offer both remote and hosted as well as “blended” services.

The benefits of either flavor of Managed Services can be compelling:

- Enforceable Service Level Agreements with financial penalties for non-compliance
- 24x7 coverage for support and problem resolution
- Ability to leverage the MSP’s broad technical expertise and best practices
- Single source of support – no finger pointing between vendors
- Faster deployment and upgrade times – days not months
- Reduce CapEx – IT delivered as a service

To read the full report, go to
www.technology-reports.com/fusionstorm.asp



FusionStorm -- "Making Technology Work" -- is a leading national provider of IT products, professional services, support contract services and 24x7 managed services for enterprises of all sizes. The company delivers complete solutions for system infrastructure, storage, networking, voice-over-IP, security, database, disaster recovery, managed hosting and remote managed services. FusionStorm offices include San Francisco (HQ), San Jose, Sacramento, Los Angeles, Las Vegas, Chicago, Cincinnati and Boston. www.fusionstorm.com • 800.228.TECH (8324).



IT SOLUTIONS 2006

Progressive Ideas and Leading Technologies

To read full reports and related information, go to the links listed below or visit www.technology-reports.com

Integrated Application Layer Firewalls Are Quickly Becoming Standard Fare

It's not just firewall proxy and port filter with stateful packet inspection kind of world any more. Over the past few years as application techniques have been refined, and applications become more sophisticated and distributed; so has the need for application traffic management. Would be villains have become equally as sophisticated in their use of tools and automated exploits; making easy work of unsuspecting application and application platforms. The ever popular search engines; have become tools of choice for attackers.

Security professionals used to be able to try to filter out bad traffic, and in some cases

check for strict adherence to published protocols and standards. Those days have been surpassed with attacks being targeted at applications, or even application platforms themselves. As web applications have become more predominant in the network; and privacy and SSL encryption has proliferated, we have lost much of our ability to watch for malicious traffic. The network traffic remains encrypted right up to the application server; in effect camouflaging the attack itself. So, repeated attempts to compromise user names and passwords go unnoticed.

A new type of appliance has taken shape. Application Traffic Managers allow for an incredible amount of control and security to be applied to security agnostic applications and appliances. New threats such as SQL injection, or parameter tampering can easily be thwarted with this next generation of traffic management appliances that take an uncharacteristic approach to security. The previous paradigm of blocking only known bad traffic has been thrown right out of the window. This new type of application traffic managers takes radically different approach; to block all but known good traffic. The appliances get deployed in to strategic positions within the network structure to decrypt and inspect at the application layer acceptable traffic patterns; and turning away all other traffic.

To read the full report, go to www.technology-reports.com/milestone.asp



Milestone Systems Inc. headquartered in Minneapolis, Minnesota is a specialized systems integration company focused on application and network high availability and security. With offices in 7 regions, and teaming with best of breed technology providers; Milestone Systems has been able to successfully architect and implement solutions for some of the most demanding customers. www.milestonesystems.com • 952.543.6999

Mix Open Source and Proprietary Solutions to Secure Your Enterprise

A secure enterprise is necessary for compliance and risk reduction, regardless of industry sector, public or private. The secure enterprise depends on a comprehensive approach to security. The elements of the secure enterprise include a security strategy based on a solid model; an architecture that fits your business; regular assessments; remediation; effective policy; real-time alerts; information integrity through log and event correlation; and identity management. All elements of the secure enterprise must be present and robust, as your enterprise is only as secure as the weakest link.

Think of your enterprise in terms of a simple model, consisting of your perimeter, network infrastructure, hosts, web application code, and people & practice. Your perimeter consists of those devices that connect the enterprise to the Internet. The perimeter is protected by firewalls, mail scanners and anti-spam technologies. Network infrastructure is all the devices and technologies that connect the inside and the outside. Hosts provide services to users, such as file servers and accounting systems. Code on your web servers gives application functionality to external users. And perhaps most important are your people and practices. Good people who know the game and who follow

best practices can overcome budget limitations and can compensate for a lack of sophisticated technologies while the strategy is implemented. The secure enterprise can be built entirely upon open source technologies, which are some of the most sophisticated available. The recommended approach is to mix open source software with proprietary devices and software.

The model ties it all together; open source and proprietary technologies help the budget; management commitment to the secure enterprise provides the traction; strategic professional services partnerships round it out. "Defense in depth" is now taking on a whole new meaning. Not only are there multiple layers of depth within a security strategy such as firewalls and IDS but there is also an emerging advantage to layering open source and strategic use of technology partnerships.

To read the full report, go to www.technology-reports.com/novacoast.asp



Novacoast is a full service IT professional services firm with practices in security, open source, and identity management. Management attention is focused on attracting the best engineering skill sets and delivering those skills to the market. Novacoast is the originator of Rapid Deployment (RDTM) methodologies. Based in Santa Barbara, CA, Novacoast has operations in eleven states and delivers services nationally. [Novacoast, Inc.](http://www.novacoast.com) • 800.949.9933 • www.novacoast.com

IT SOLUTIONS 2006
 For in-depth reports on these
 and other technology topics, visit
www.technology-reports.com



To read full reports and related information, go to the links listed below or visit www.technology-reports.com

Five Strategies to Maximize the Business Value of Future IT Investments

In anticipation of the widespread adoption of new technologies – from virtualization to low powered, multi-core 32-bit/64-bit platforms – today's enterprise infrastructures are undergoing a significant transformation. Where yesterday's enterprise infrastructure accommodated a large number of servers, filled with home-grown and commercial applications in a fairly complex computing environment, Next Generation Enterprise Infrastructures will be forced to meet the increasing user demand for applications driven by SOA models and Web Services technologies while simultaneously attempting to do more with less.

Transforming your existing infrastructure to a next

generation model will require careful planning and a thoughtful, strategic approach. That includes a detailed analysis of the "five strategies" most important for maximizing the business value of IT investments:

1. Recognize that it's not enough to have the fastest and most robust hardware. The software applications that you use to run your business and interface with your customers generate the most value for your organization.

2. Make a distinction between revenue-generating and administrative support applications. Back-end applications and administrative tools may be important to keeping operations running smoothly but it is the commerce functions and customer support systems

that determine your ability to collect revenues.

3. Set a plan for critical path monitoring to identify which applications should be keeping you up at night. Legacy monitoring systems can't distinguish between mission critical and non-essential applications. Organizations need monitoring solutions that alert IT managers only to serious problems impacting performance of customer-facing and operations applications.

4. Align system and application performance metrics with business metrics -- and get everyone from IT to LOB managers on the same scorecard.

5. Establish a plan to guard against security threats and generate audit trails to meet regulatory requirements. Capturing comprehensive application metrics for analysis now or later are keys to managing the infrastructure securely.

To read the full report, go to www.technology-reports.com/rto.asp



RTO Software is a leading provider of application performance monitoring and acceleration solutions. RTO offers extensive capabilities to enterprises that need performance monitoring and acceleration of a wide range of applications in their real-time, business-critical infrastructure to deliver consistently superior user experiences. RTO has more than 400 customers worldwide and its solutions are in use in many industries, including financial services, healthcare, media and entertainment, e-business, telecommunications and government. <http://www.rtosoft.com> • 866-987-2900

Email, IM, Web and VoIP Converge: Are You Secure and Compliant?

Convergence, we have all heard it, but what does it really mean for businesses today? Convergence enables users to consolidate their traditional and IP-based communications -- Email, IM, Web and VoIP -- on a single device or application. Early examples include Microsoft's® Exchange, LCS, and SharePoint that provide an integrated platform for IP communications. In the handset world, the BlackBerry® and smart phones have evolved to provide users with a single device to meet all their communications needs.

This convergence of technology opens the door to new opportunities in communications, but

also introduces new security concerns. A converging threat landscape brings the risk of multiple attacks while also the need to ensure corporate, regulatory compliance and privacy requirements are met. As new blended threats emerge such as virus infected messages used in spam campaigns it is critical to enforce a single policy across all IP communications. Organizations can no longer rely on conventional point products and reactive threat prevention services to secure their networks and meet compliance and privacy requirements. Added to this is the additional strain of new complexities where information can

be sent and received over multiple IP communications channels simultaneously.

"Threats are changing and business communications are using more and more network protocols. Enterprises need next generation security solutions that efficiently and effectively protect all communications channels," said John Pescatore, Vice President and Distinguished Analyst of Gartner, Inc.

Bottom line: In order to be secure and compliant, organizations need a single content security platform to prevent attacks, block unwanted content, control confidential and private information, and manage the messaging infrastructure centrally, across all IP communications -- Email, IM, Web and VoIP.

To read the full report, go to www.technology-reports.com/borderware.asp



BorderWare Technologies makes Internet communications safe. The company is the leading provider of content and application security that secures business-critical applications including Email, Instant Messaging, Web and Voice over IP. For over 12 years, BorderWare has helped organizations mitigate business risk by: reducing the complexity of a multi-vendor security environment; ensuring business continuity; and reducing exposure to legal liability by ensuring corporate and regulatory compliance and privacy requirements are met. 877-814-7900 • www.borderware.com



IT SOLUTIONS 2006

Progressive Ideas and Leading Technologies

To read full reports and related information, go to the links listed below or visit www.technology-reports.com

The Best Defense is a Good Offense

Today's cyber-threat environment is increasingly severe, over 90% of companies have anti-virus, anti-spam and firewall defenses, but attacks and malware are still getting through. Additionally, the threat is increasing from the inside-out. Challenges posed by this are both financial and operational. Financially, organizations are legally liable for sensitive data, stock prices get impacted upon disclosure, revenue systems are disrupted, and human 'firefighting' creates unnecessary expense to fix. Operationally, the IT department doesn't add value, business services are disrupted, and employee confidence reduced. What is needed is a new type of security element that

pervades the network and automatically protects organizations from a broad variety of attack types (e.g., worms, viruses, Trojans, DDoS, Spyware) and from all potential points of attack.

Intrusion Prevention Systems (IPS) are the best step in this direction. In the simplest sense, an IPS is a computer appliance that blocks attacks before they can reach their target. In a broader sense, an IPS performs total network packet flow inspection, with deep analysis and classification by receiving constant security filter updates to protect against threats.

Security effectiveness is measured in three dimensions: accuracy, coverage, and timeliness. Of

these, accuracy is the most important. Accuracy ensures malicious traffic is blocked, and legitimate traffic is not. Coverage refers to the breadth of attacks or attack vectors that an Intrusion Prevention System can protect against. Timeliness is the speed with which an IPS offers protection against a new threat. If filters are in place, they can protect an organization preemptively before the existence of an exploit or worm.

IPS represents a philosophical shift from traditional reactive security tools like firewalls and intrusion detection systems that require extensive configuration, tuning and manual maintenance, to an automated security solution. Therefore, organizations should heed what doctors often say "the best form of defense is prevention".

To read the full report, go to www.technology-reports.com/tippingpoint.asp



TippingPoint is the leading provider of network-based intrusion prevention systems with innovative features including spyware protection, quarantine protection, phishing protection and multi-gigabit throughput. TippingPoint's IPS offers accurate, automatic blocking of malicious traffic, VoIP security, bandwidth management and centralized management to all types of enterprise, government, and education organizations. Austin, TX • 512 681 8000 • www.tippingpoint.com

Electronic Discovery Systems Meet New Legal and Technological Needs

Many of the major lawsuits recently in the press require the review of volumes of data greater than is stored in the Library of Congress; many lesser-known cases go to similar extremes. As litigation and government investigations grow in number and complexity, so grows the amount of material that has to be reviewed during discovery.

Choosing the right discovery solution is critical for corporations to manage costs and control risk. If the wrong choice is made, documents may not be available for review, be in the wrong format, or have been corrupted; the larger the scope of discovery, the larger the risk. Because of the tight

deadlines involved with discovery, it's no longer practical to wait for a subpoena before putting a document discovery process in place. Many organizations are building powerful electronic discovery systems and processes into everyday operations in order to minimize the impact to their business when a document request is received.

Implementing an e-discovery system into normal business practices and the document life cycle management also helps manage costs. Such a system identifies and stores documents in a sensible, comprehensive manner that reduces risk of adverse outcomes; reduces confusion by putting

operational, legal and technical personnel on the same page; and lowers costs by preventing duplication of review work.

Ideally, each relevant document should be processed only once, even when it bears on multiple cases. Documents should be accessible to multiple authorized parties, and displayed in a single format within an intuitive interface that makes the system easy to use.

Today, the risks of not having an e-discovery system are greater than the cost of implementing one. Discovery preparedness can make or break a company's future, and more companies are turning to full-service providers for comprehensive solutions.

To read the full report, go to www.technology-reports.com/LexisNexis.asp



LexisNexis® Applied Discovery® - For complete e-discovery services trusted by the nations top law firms and corporations. Applied Discovery provides the solution that captures over 99% of critical documents to manage litigation risks and control costs. LexisNexis® (www.lexisnexis.com) is a leading provider of information and services solutions to a wide range of professionals in the legal, risk management, corporate, government, law enforcement, accounting and academic markets.