

October 2007

Vol.1/Issue 3

## Ecora Opens New Office in Massachusetts

*Strong revenue growth, increased industry need for configuration and compliance tools fuels company expansion*

Leveraging strong business performance and an array of new customers, Ecora has opened a new office in Burlington, Massachusetts, allowing the company to accommodate its rapid growth and attract additional high-technology talent. The new office is located at One Burlington Business Center, 67 South Bedford Street, Suite 301E, Burlington, Massachusetts, 01803.

“We are already reaping benefits from this new office,” said Michael Sullivan, Ecora president and CFO. “We have been able to attract key sales and services personnel by having a Massachusetts location. As we continue to execute on our

plans to expand these areas over the coming months, it allows access to top talent, and gives us the ability to better service both our new and existing customers.”

Ecora’s sales in the first half of 2007 are up 21 percent over the comparable period in 2006, excluding one-time items. For the quarter ended June 30, 2007, 33 new customers were added. Sales for the quarter were up 21 percent over the prior quarter and up 29 percent over Q2 2006.

“Sarbanes-Oxley and the Payment Card Industry (PCI) Data Security Standard have made compliance

more of a priority for many companies,” continued Sullivan. “Ecora’s business is built on providing our customers with the data they need concerning their IT infrastructure in order to analyze and demonstrate their compliance not only with government regulations, but also with IT best practices, resulting in improved operations.”



## Reining in the Effects of Uncontrolled Change

*Why controlling change can ensure security, compliance, and operational effectiveness*

In IT management, as in business as a whole, change is a constant, and can range from the planned, such as application and operating system upgrades, patch installations, and approved configuration updates, to the unplanned, including accidental system alterations and malicious security breaches. Not surprisingly, these “unplanned” changes can have the greatest impact on the organization. In fact, Enterprise Management Associates (EMA) estimates that, on average, more than 60 percent of all critical system and application outages are caused by inappropriate changes.

The costs associated with unplanned and uncontrolled change can be significant and can impact an organization’s customer service, security, compliance, and administration. For example, unplanned and uncontrolled change can lead to a higher time-to-

value for new products and services, inconsistent and unpredictable service, increased security and compliance risks, and higher administrative costs.

Yet, if nothing changes or evolves within an enterprise, an organization can fall behind as competitors take the lead in the market. The key is to implement processes and procedures to manage and control change.

### Identifying Planned and Unplanned Change in the Infrastructure

By identifying authorized changes and detecting unauthorized changes quickly, organizations can ensure quick problem resolution and control costs. A recent EMA study showed that, on average, problem resolution can take between one and four hours, with a significant part of the delay—between 30 minutes and two

hours—dedicated to simply detecting and identifying the changes that caused the problem in the first place. Reducing this time is essential; in the time it takes to detect and resolve an issue, service and availability levels can be impacted and frustrated customers may already have given up.

There are a number of reasons that detecting change can be such a challenge. The first is the complexity of today’s IT implementations. The complexity of IT infrastructures contributes significantly to the second reason that detecting change can be such a challenge: an organization’s lack of visibility into change.

So how do most organizations detect unplanned change? In an EMA survey, 18 percent of respondents indicated that they learned about unplanned change after an

### SC Magazine Awards

2

Vote for Ecora Auditor Pro as Best Audit/Vulnerability Assessment Solution in 2008 SC Magazine Awards...

### You Can Survive a PCI-DSS Assessment

An Ecora primer for QSAs on best practices for overcoming challenges and achieving compliance ...

### Update on Ecora’s Self-Service Support Portal

3

Search Ecora knowledgebase, submit or review cases—quickly and easily ...

### Ecora Professional Service Offerings Add Further Value to Auditor Pro

Ecora provides our customers with complete solutions to meet their demands for controlling change and delivering auditable evidence for compliance validation

### Tecnológico de Monterrey

4

Mexico’s largest private university looks to Ecora to improve system availability, shorten problem resolution...

### “Automated Documentation and Compliance”

Ecora’s Bryan Cote featured in the Realtime Windows Server Podcast Series...

## SC Magazine Awards

Select Ecora Auditor Pro as Best Audit/Vulnerability Assessment Solution in 2008 SC Magazine Awards

The 2008 SC Magazine Awards celebrate the best products, services and security teams in the industry today and Ecora Auditor Pro is one of a handful of companies nominated for Best Audit/Vulnerability Assessment Solution.

As a user of information security products and services, you and your colleagues are eligible to vote and, at the same time, help recognize Ecora Auditor Pro as a solution that has proven its worth in addressing the IT challenges you face every day.

Voting is now open and will close on November 2nd.

If you believe in the value Ecora Auditor Pro has brought to you and your organization, please give it your vote, and help it be a winner.

To vote [click here](#)



## You Can Survive a PCI-DSS Assessment

*An Ecora primer for QSAs on best practices for overcoming challenges and achieving compliance*

The most common challenges to ensuring PCI compliance include protecting and managing data, controlling change, and auditing and enforcing policies, but there are a number of best practices that can help to ensure that infrastructure components are secure prior to a PCI assessment. These best practices are summarized by category below.

### Firewalls and Routers

- Secure firewalls at each Internet connection, demilitarized network zone, and the internal network zone. Deny all unnecessary traffic, particularly outbound traffic, for any systems that process or store cardholder data. Ensure that firewall rule sets are as granular as possible. Importantly, track all changes.
- Use appropriate firewall protocols: inbound HTTP, HTTPS to web servers, SMTP to mail server, and SSH/IPSec.
- Look to standard router configurations so all routers have a consistent build.

### Servers and Workstations

- Build secure systems. Document build standards and ensure that they are repeatable. Change defaults and harden servers by disabling unnecessary services. Ensure that anti-virus and anti-spyware software is in place on all servers.
- Deploy a secure and effective patch management strategy.
- Ensure security testing and validation. Run regular vulnerability scans; PCI requires quarterly scans, but a true best practice is to scan more frequently. Scan all systems prior to release to production.
- Monitor all pertinent system activity, including securing and managing system event logs, proactively detecting intruder activities, and monitoring file integrity.

### Transmission of Cardholder Data

- Ensure strong encryption protocols: SSL, IPSEC, private WAN (e.g., Frame Relay), and SFTP.
- Implement a strong encryption strategy, particularly for wireless networks.
- Ensure email encryption configuration and management. Ensure that there is a genuine business need to send full credit card numbers via email, and whenever possible, do not email the full PAN.

### Wireless and POS Devices

- Ensure consistent monitoring. Wireless should only be used to transmit cardholder data when absolutely necessary. Change default configurations, use strong key encryption, and deploy a wireless IDS/IPS. Finally, wireless access points should be physically secured.

### Application Development

- Deploy controls commensurate with the data to be protected. Segregate the development/test environment and the production environment.
- Integrate change management, testing, and promotion into production strategies to ensure approval by appropriate stakeholders and that all changes are tracked.
- Mitigate application-level security vulnerabilities by deploying secure coding best practices, thorough code review, and application-level penetration testing to close the loop. In 2008, PCI-DSS Requirement 6.6 will mandate third-party code review or an application-level firewall.

### Access Control and Management

- Manage access through a formalized process to request authorization, and periodically review the authorized user list and access list to find changes.
- Ensure the timely removal of terminated users.



- Implement frequent review of user access.

### Monitoring and Testing

- Implement a systems' monitoring strategy that provides audit and accountability, including a centralized log server that records who, what, when, and where that is reviewed regularly.
- Secure audit trails and log files in a centralized log server, accessible only on a need-to-know basis.

### Testing Policies and Procedures

- Use port scans, vulnerability scans, and penetration testing based on requirements.

### Data Protection

- Eliminate and purge data when it is no longer needed. Keep cardholder data only for the length of time required for the business.
- Send only relevant data to internal customers.

### Leveraging Automation to Develop an Automated PCI Compliance Process

Given the gap between growing compliance requirements and flat IT budgets, organizations are looking to automate the compliance process. In fact, many of the best practices cited above can be accomplished more efficiently and effectively through automated processes. A recent *InformationWeek* study indicated that "organizations with the fewest compliance problems are spending nine percent more to automate

*continued page 3*

## Update on Ecora's Self-Service Support Portal

Search Ecora knowledgebase, submit or review cases—quickly and easily

Ecora's Self-Service Support Portal continues to grow in both content and use.

Here are some interesting facts about the Portal:

- There are more than 400 knowledgebase solutions
- Over 370 users are registered and using the portal
- Over 200 knowledgebase searches are conducted on average each month
- An additional 50 articles are added to the knowledgebase monthly

The Self-Service Support Portal provides you with an easy-to-use online tool to search the solutions knowledgebase, log support calls, and interface with Ecora support personnel to resolve your issue. Using the Portal also gives you a history of your support tickets and solutions.

The Ecora Self-Service Support Portal is available to customers with valid maintenance and support contracts. To access the portal, [click here](#), and then click on the **Support Portal** link. To request access to the portal, [click here](#), or contact your Ecora sales representative for more information. Customers under a trial are not permitted access to the Portal and should continue to submit questions using the online [submit form](#).

## Ecora Professional Service Offerings Add Further Value to Auditor Pro

Ecora provides our customers with complete solutions to meet their demands for controlling change and delivering auditable evidence for compliance validation. Given each customer's unique business requirements, resource availability, and priorities, Ecora provides a suite of professional services to help our customers increase the value of their Ecora software solutions:

### Rapid-Remote

Ecora understands that some of its clients would prefer to implement the product on their own and receive guidance and training via remote methods. Ecora's Rapid-Remote service combines web-conference training and consulting to provide you with the information you need to address your IT issues and achieve a rapid return on your investment.

With Ecora Rapid-Remote services, we will:

- Assist with the proper implementation and configuration of your software
- Properly educate users on the basic operation of the software

### Implementation & Training

Ecora Implementation & Training services combine on-site consult-

ing, customization, and training to provide you with solutions to your problems and the training you need to achieve a rapid return on your investment. With our Implementation & Training services, our goal is to enable you to become self-sufficient and proficient in the use of the software in the shortest amount of time.

With Ecora Implementation & Training services, we will:

- Assess your needs and develop an appropriate implementation plan
- Implement the optimal system for collection and reporting in your environment
- Provide a thorough understanding of the rich report templates and pre-determined policies to ensure a rapid return on investment
- Properly educate users on the operation of the software

### Custom Reporting

The Custom Reporting service leverages best practices garnered from over 800 active worldwide customers with environments from large and complex to small and straightforward. Ecora uses this experience combined with the expertise of our own IT professionals to help you customize and gen-



erate the reports you need to:

- Validate and sustain compliance to regulatory and industry standards
- Strengthen your change and configuration management process
- Improve and enforce your security standards
- Maximize system performance and availability
- Maintain current system documentation to retain critical knowledge
- Prepare for disaster recovery and enhance business continuity planning

### Health Check

IT environments are in constant evolution. Technology is added or removed. Administrative expertise is reallocated. Business drivers that

*continued page 5*

## You Can Survive a PCI-DSS Assessment

*continued from page 2*

audit functions and 11 percent less on contractors and outside services" (*InformationWeek*, December 4, 2006).

### Preparing for PCI—before an Assessment Begins

Ecora provides software and services that allow organizations to implement sustainable, automated PCI compliance programs.

To view the webinar "You Can Survive a PCI-DSS Assessment" on demand, [click here](#). To download the whitepaper, [click here](#).

## “Automated Documentation and Compliance”

Ecora’s Bryan Cote featured in the Realtime Windows Server Podcast Series

Recently, Realtime Windows Server Community Resident Editor Greg Shields, MCSE: Security, CCEA, sat down with Bryan Cote, senior product manager at Ecora Software, to discuss the state of compliance. The two identified some of the challenges associated with network documentation and compliance and how Ecora Auditor Pro resolves some of the critical missing auditing pieces in native operating systems, including:

- Understanding data collection requirements to meet a range of compliance regulations
- Using automation to manage enterprise security information
- Leveraging automation to inventory and update asset databases
- Integrating data with automated remediation tools

“Understanding your network is one thing, but proving that you are controlling it is another thing entirely.” With compliance regulations requiring a database of record showing what on your network changed and when, it is growing more impossible every day to fulfill the needs of documenting and auditing your environment,” said Shields. “That’s why tools like Ecora Auditor Pro exist. Inventorying and storing thousands of elements about every machine on your network, this toolset means you can pass compliance audits with ease. All the while, you get a better running network because you have more information about that network.”

*continued page 5*

## Tecnológico de Monterrey

*Mexico’s largest private university looks to Ecora to improve system availability, shorten problem resolution*

Founded in 1943, Tecnológico de Monterrey is a private educational institution consisting of 33 regional campuses, with headquarters in Monterrey City. Today, there are more than 90,000 students across the institution’s campuses, as well as additional students in other academic centers throughout Mexico and Latin America.

In 2007, for the fourth year in a row, Tecnológico de Monterrey was named one of Mexico’s top 50 most innovative organizations by *InformationWeek*, and, in 2006, the *Wall Street Journal’s* survey of corporate recruiters ranked the institute’s business school as number seven in the international business school category, which included North American, Latin American, and European universities.

### Controlling Change; Preventing Downtime

With campuses widely dispersed across Mexico and offices around the globe, thousands of users, and a complex multivendor environment, Tecnológico de Monterrey’s infrastructure more closely resembles that of a global business enterprise than that of a traditional educational institution. To help ensure control of the expansive environment, primary IT resources are centralized on the Monterrey campus, with regional IT departments

accountable for local services. “Even with a clear differentiation of duties, controlling changes throughout our environment has been a challenge,” explained Ramses Herrera, director of infrastructure administration and operations. “We’ve had to trust that our entire staff was doing what they were supposed to do and, if a problem arose, we had to question everyone to determine what had changed and who had changed it. This manual process frequently took days to conduct, and was especially problematic when critical business services were interrupted as a result.”

Maintaining up-to-date documentation was also a challenge for Tecnológico de Monterrey. “Having system documentation that was up to date depended on the willingness of our IT staff to make the effort manually,” Herrera said. “As you can imagine, documenting all our IT systems and tracking and controlling configuration changes manually was highly inefficient.”

Tecnológico de Monterrey needed a comprehensive tool that would enable them to ensure change control validation, prevent unplanned downtime, and automate documentation. The answer was Ecora Auditor Professional.

*“In a single, comprehensive solution, Auditor Professional gave us everything we needed: complete system documentation generated automatically and a clear way to identify authorized and unauthorized system changes quickly. In addition, the solution is literally plug and play; we began using Auditor Pro almost immediately”*

— Ramses Herrera Director of Infrastructure, Administration, and Operations Tecnológico de Monterrey

## CUSTOMER SPOTLIGHT



[Click here](#) to read full Case Study.

### Proven Technology in a Comprehensive, Plug-and-Play Solution

“We selected Ecora Auditor Professional for a number of reasons,” explained Herrera. “In a single, comprehensive solution, Auditor Pro gave us everything we needed: complete system documentation we can generate automatically that identifies authorized and unauthorized system changes quickly and clearly. We had looked at other solutions but they appeared much more complex.”

Today, Ecora Auditor Professional is enabling Tecnológico de Monterrey to address problems that had been associated with tracking changes manually.

Dealing with any unplanned downtime is also simplified with Ecora Auditor Pro in place. “In the past, if downtime occurred, we had to go through literally thousands of changes to identify what was different between time A and time B.”

*continued page 5*

## Tecnológico de Monterrey

*continued from page 4*

Herrera said. “With Auditor Pro, we have detailed change reporting that lets us proactively identify if changes could cause problems with performance, and, if downtime does occur, Auditor Pro identifies configuration changes to help us identify the root cause of the problem promptly.”

### Up-To-Date Documentation Enhances Control

Auditor Pro’s auto discovery feature identifies systems, servers, services, applications, and devices throughout the Tecnológico de Monterrey environment to provide an accurate infrastructure inventory. “Auditor Pro gives us complete visibility into our extensive infrastructure,” Herrera said. “At any given point in time, we can now have a complete infrastructure inventory, which ensures we have greater control of everything we manage.”

[Click here](#) to read full Case Study.

## “Automated Documentation and Compliance”

*continued from page 4*

During the interview, Cote cites an Ecora customer who credits Auditor Pro with reducing their time to problem resolution by almost a half. “This is really at the heart of what Ecora enables our customers do,” Cote said. “We eliminate the complexity and the challenges of collecting data and then provide reporting tools to ensure that the data can be used to meet business requirement.”

[Click here](#) to download the podcast.

## Ecora Professional Service Offerings Add Further Value to Auditor Pro

*continued from page 3*

force an organizational realignment can have an adverse effect on IT services that could negatively impact the business. In each case, adjustments to the configuration of Ecora Auditor software may be required to assure maximum value continued to be provided. In addition, the information you initially needed to collect and report on may not be the information you require now. New compliance regulations and evolving IT best practice frameworks continually increase the scope of work your IT organization must undertake to properly understand and manage your environment.

For these reasons, it is important to periodically review your Ecora Auditor implementation to ensure

that data collections and reports are adjusted to assure they are providing all of the information that is important to the organization. An Ecora Health Check is a cost-effective way to guarantee that value is continuously realized from your investment. Based on your particular requirements, Ecora’s Health Check Service can be delivered remotely or on-site with services tailored to fit your specific business and operational needs.

With Ecora’s Health Check services, we will:

- Ensure your software is deployed and functioning properly
- Analyze discovery and collection methods
- Provide a comprehensive review

of policies and reports

- Validate users are properly educated on the basic operation of the software
- Offer recommendations of how to get greater business value from your Ecora investment

Regardless of whether you need additional resources, services, or advice to efficiently and accurately integrate Ecora’s software into your existing IT infrastructure, Ecora has a services solution to meet your requirements.

Please contact your Ecora account executive, [sales@ecora.com](mailto:sales@ecora.com), or [ProfessionalServices@ecora.com](mailto:ProfessionalServices@ecora.com) to learn more.

## Reining in the Effects of Uncontrolled Change

*continued from page 1*

outage or slowdown and an additional 24 percent said they detected unplanned changes manually. In both cases, it is likely that the organization was suffering the effects of the unplanned change—particularly in terms of reduced availability and increased costs—before the problem was detected.

### Implementing an Effective Automated Change and Configuration Management Solution

An effective change and configuration management (CCM) strategy ensures that control is maintained over an IT infrastructure, and a successful automated change and configuration management solution must meet several key criteria. First, it should offer a single, centralized interface for identifying all configuration elements across an IT infrastructure. It should also deliver powerful reporting capabilities that provide a high-level status of overall enterprise health.

In addition, an automated CCM solution should enable an organization to validate that changes have been made, which closes the loop on the change request process.

### Addressing Security and Compliance with Change and Configuration Management

In an EMA survey, nearly 100 percent of respondents indicated that a change and configuration management solution was either “critical” or “important” to ensuring security and compliance.

Change and configuration management unifies compliance and security to ensure strict control over the critical IT infrastructure. With an automated CCM solution in place, organizations can simplify the process for meeting audit requirements. Plus, CCM ensures data and access security through visibility and control over all IT assets, configuration control to prevent unauthorized access, and the capability to identify, remediate, and prevent exposures.

Finally, CCM ensures security and compliance best practices for automated detection and remediation, compliance checking, and continuous compliance reporting.

### Change and Configuration Management with Ecora Software

Ecora is a leader in enterprise-wide

change and configuration reporting solutions that address a pervasive problem—the lack of visibility into configuration changes across the organization. Ecora’s Auditor Pro provides out-of-the-box reporting functionality that enables organizations to resolve IT service management and compliance issues efficiently and effectively. Auditor Pro collects configuration data from across the infrastructure, including operating systems, database management systems, directory services, and applications, and presents reports customized for particular business needs through a centralized, web-based console.

If you implement processes and policies for sound configuration and change management, you will realize improved Quality of Service, reduced downtime, satisfied customers, and a more profitable organization.

To view the webinar “Reining in the Effects of Uncontrolled Change” on demand, [click here](#). To download the whitepaper, [click here](#).