

CA Advisor

SECURITY MANAGEMENT NEWSLETTER

February 2009

How Role Management Can Help Reduce IT Costs

A Q&A with Dr. Ron Rymon

Today's major IT governance initiatives often require effective management of access rights and



privileges. Role-based management provides the best practices for doing so and at the same time is evolving to influence more facets of IT processes. To find out more about these changes, we met with Dr. Ron Rymon, an early pioneer in role provisioning and the founder of Eurekify, a leading provider of privilege, role and policy management solutions recently acquired by CA. Rymon is currently the vice president of business unit strategy for CA's Security Management business unit. What follows is the first of a three-part interview with Dr. Rymon on the present and future of role-based management.

Q: Let's start out by defining what you mean by role-based management.

A: Roles represent the DNA of an organization, and role management is about rationalization of access rights (and possibly other IT and business resources) based on a clear model of business needs, practices and other considerations. For example, one role may define the access rights needed to perform a certain part of a business process, such as a paying a vendor. Another role may define the access rights typically granted to a certain employee type. With a good role model, organizations do not have to invest the time and resources in determining and assigning access rights for each IT resource every time they hire new employees or change an employee's responsibilities to meet new business mandates. Role management is also critical to automated verification of compliance with regulations and other organizational policies and practices. Consulting with the organizational

role model may provide recommendations and other decision-support information in many other business processes, making them a lot smarter and more productive.

Q: You refer to a "good role model." What barriers must organizations confront when creating an effective role model?

A: The first challenge is the creation of an effective role model that fits the organization and its anticipated use, covering 70 to 80 percent of all access rights. Many organizations were led to believe that they could do so through a process-based approach, based on interviews and top-down construction from first principles. Unfortunately, this works for the first 20 to 50 roles, but then this approach becomes more and more intractable, until it finally breaks. A more effective approach leverages existing privileges information to guide you in the creation and management of the role model over time. Using this technology is the only way to scale role management in organizations with many thousands of users, hundreds of systems and millions of access rights.

Q: Can you be more specific?

A: We found that you could use existing access rights, combined with accepted business structures and concepts, such as org chart and reporting structures, to provide very valuable cues and shortcuts towards the creation of a proper role model. So we developed advanced pattern-recognition software that used these cues (extracted through a mining process) to guide in creation and ongoing management of effective role models. This is the only approach that we know of which allows large companies to quickly create and maintain role models covering 70 to 80 percent of all access rights and practical for a variety of provisioning and compliance applications. All other

approaches take a lot longer, fail more often and are usually not completed.

Q: In the past year or two there has been a sharp increase in the demand for role management. What do you attribute this to?

A: Identity Management (IdM) solutions (especially automated provisioning) are reaching maturity, and customers are finding that role-based management is key to effective implementations. As organizations deploy IdM solutions and the process is made efficient, business people are finding it difficult to participate in them without business-oriented role definitions that logically package IT-oriented access rights. At the same time, companies that were relying solely on a process-based approach to define roles found that it was difficult, expensive and often lead to inconsistencies. The need for compliance has also increased the need for automated verification of access rights.

Q: Recognizing that every organization is unique and different, how would someone start in this whole role-management process?

A: First, start with a short survey which has an initial goal of understanding and quantifying the existing issues, identifying opportunities (especially quick wins) and building a solid business case for the project. The second goal is to create an implementation plan that would be feasible, acceptable to all players and stake holders and technically achievable in a reasonable time and cost. This can only be done through an analysis of the existing authorization structures and through review of alternative implementation approaches.

With Eurekify's pattern-recognition technology, such a survey can usually be started and finished in only one to two weeks, including comprehensive analysis of existing access rights, identification of issues and opportunities for improvement; simulation of 10 to 15 alternative role modeling approaches, to identify the one that best fits the organization, both technically and from a business perspective; review of compliance with top policies such as Segregation of Duties (SoD) and other restrictions.

Q: How does someone attack a role-management project?

A: The survey provides ample information for planning a role-management project. Beyond that survey, however, the project usually takes the following steps:

1. Aggregation of authorization data from many systems and applications
2. Initial cleanup consisting of easiest privileges-quality improvements and most flagrant compliance issues
3. Creation and approval of a role model and instantiation of ongoing role-management processes.
4. Creation of a compliance-verification process.

Q: So you've outlined the process—now where does a Eurekify customer use your technology in the process?

A: Eurekify's pattern-recognition technology is key to all steps of the project. Let me give you some examples: Creation and ongoing management of an effective role model is next to impossible, or else terribly expensive, without our pattern-recognition technology. Compliance and governance processes are also extremely laborious and highly inconsistent without proper automation of compliance and risk-management principles. Finally, quality management is also an extremely laborious task without technology that can automatically detect deviations and out-of-pattern exceptions.

In the second part of our interview, Dr. Rymon will explain how Identity Compliance can be transformed from a cost center to a tool that improves access request and approval processes while minimizing organizational risk.

Currently the Vice President of business unit strategy for CA Security Management, Dr. Ron Rymon founded Eurekify in 2002, and is an expert in the strategic and tactical application of data-driven modeling techniques. Prior to founding Eurekify, Dr. Rymon founded and managed CrediView, developer of fraud detection and prevention solutions for Internet merchants. Dr. Rymon is the author of a novel data mining and modeling technique that has been scientifically shown to generalize and improve upon state-of-the-art technologies. In collaboration with the best domain experts, Dr. Rymon successfully applied this technology to a number of scientific problems, as well as business applications in marketing, financial modeling, and insurance risk. Dr. Rymon has consulted extensively with large U.S. and overseas corporations and government agencies. Dr. Rymon holds a PhD in Computer Science from the University of Pennsylvania (1993), and has been on the research faculty of the University of Pittsburgh, and the

For the latest issue of CA Advisor: Security Management Newsletter, visit ca.com/newsletters/secure. To subscribe to receive future issues, or to manage your preferences, visit the [CA Preference Center](#).



Interdisciplinary Center in Herzliya, Israel. He published extensively in scientific journals and conferences.

For the latest issue of CA Advisor: Security Management Newsletter, visit ca.com/newsletters/secure. To subscribe to receive future issues, or to manage your preferences, visit the [CA Preference Center](#).