



The Security Division of EMC

White paper

Counting the Costs

Addressing the Cost of Compliance



Understanding the true cost of compliance

Increasing governmental, industry, partner/customer and internal requirements are tasking organizations to address an ever-widening range of compliance requirements. At the same time economic considerations continue to limit how much organizations are able to spend on the people,

processes and technology necessary to meet those requirements. This paper discusses how organizations can develop and maintain a true understanding of the cost of compliance as well as approaches that can help reduce those costs.

Contents

I.	Executive Summary	page 1
II.	Introduction	page 1
	Compliance	page 2
	Audience	page 2
III.	Understanding the Cost of Compliance	page 2
	Types of Costs	page 2
	Documenting Costs	page 3
IV.	Managing the Cost of Compliance	page 4
	A Framework-based Approach	page 5
	Sustainable Compliance	page 7
	Other Measures	page 7
	Automation	page 7
	Vendor Support	page 8
	Infrastructure Consolidation	page 8
V.	Summary	page 9
	References	page 9
	About RSA	page 10
	About the Author	page 10

I. Executive Summary

Organizations face the daunting task of maintaining compliance with an ever-increasing range of internal and external requirements, while at the same time ever-changing economic conditions force these organizations to maintain or even reduce the cost allocated towards compliance. Taking a structured approach to analyzing and understanding the actual cost of compliance across the entire organization can greatly simplify the task of identifying possible areas of improvement. Once these areas are identified, a standards-based framework approach to implementing compliance-related technologies can potentially result in the elimination of significant areas of redundant costs. Other areas that may help in reducing costs include replacing expensive manual processes with automated tools, encouraging vendors to integrate support for compliance capabilities into their products, and consolidating the infrastructure to reduce the number of points of compliance management.

II. Introduction

In today's environment, security professionals are being tasked to address an ever-increasing range of requirements with a constantly growing array of threats, while at the same time being asked to maintain or even reduce costs. Like Hans Brinker with his finger in the dike, these staff are asked to stop more and more leaks but are quickly running out of fingers (and toes) needed to fill those gaps. In order to hold back the flood waters, security professionals need to understand exactly what holes exist, what resources are being used to plug them, and what they can do address the problem on an on-going basis with limited resources.

Organizations must maintain compliance while being tasked by an ever-increasing range of requirements from partners, customers and internal sources.

What are the factors driving the increasing need for security resources? Some of the primary cost drivers that security and compliance professionals are facing include:

- **Increasing regulatory requirements.** No one believes that the regulatory environment organizations must address will be simplified any time soon. Governments and industry organizations continue to develop new standards and regulations, while at the same time expanding enforcement of existing ones.
- **Increasing internal, partner & customer requirements.** In addition to external government and industry requirements, organizations are being tasked by an ever-increasing range of requirements from partners, customers and internal sources. The result is that virtually every new type of information introduced into an IT infrastructure has multiple compliance requirements associated with it.
- **Increasing information volume.** Very few (if any) organizations can claim that the volume of information they create, store and manage has decreased in recent years. Organizations continue to add new sources of information, much of which is sensitive and needs to be protected.
- **Increasing infrastructure complexity.** As with information, very few organizations have an IT infrastructure that remains static. As new servers, networks, databases, storage systems and applications are added, the scope of security operations must be expanded to protect them.
- **Increasing threat environment.** The range and complexity of the threats faced by an organization changes on an almost daily basis. New, more sophisticated attacks are coming from all directions, including from inside the organization itself.

In order to address these drivers in a cost-effective manner, security professionals must understand the true costs associated with their compliance efforts, and develop an approach to adequately address compliance that minimizes costs while still meeting requirements.

It is important to note that this paper focuses exclusively on cost, not value. While understanding both cost and value (e.g., return on investment) is critical when making decisions related to compliance, the starting point is gaining a comprehensive understanding of the complete costs associated with compliance spending. Even though most organizations have methodologies for understanding risk and the resulting value of security and compliance spending, economic factors frequently force cost factors to take a higher priority.

Compliance

The word ‘compliance’ is used extensively throughout this paper; while ‘compliance’ is frequently used to refer to the process of meeting requirements defined by formal government and industry regulations, RSA believes that this definition is too limited in scope. More importantly, the artificial separation of regulatory/industry compliance from other aspects of an organization’s security program inevitably leads to increased costs. Consider all of the drivers that results in an organization devoting resources to security:

- **Government regulations**, e.g., SOX, HIPAA, EU Data Privacy Directive, etc. (the traditional domain of ‘compliance’)
- **Industry regulations**, e.g., PCI, NERC, etc.
- **Partner requirements** – security requirements levied upon an organization by any partners they deal with
- **Customer requirements** – security requirements levied upon an organization by their customers, citizens, etc.
- **Internal requirements** – internal security requirements defined by an organization itself, frequently by a security policy

While these different drivers are frequently handled by multiple groups with potentially different approaches and goals within an organization, the reality is that they all result in the same thing – specific requirements being defined that must be met by implementing security controls. By taking a consolidated view of the people, processes and technologies necessary to address these various requirements, organizations can accrue many

benefits, including reduced costs (discussed in this paper) and improved overall security. To this end, the word ‘compliance’ is used in this paper to refer to the process of meeting any security requirement, regardless of its origination.

Audience

This paper is targeted at security, legal and compliance professionals that are responsible for understanding and managing security- and compliance-related costs within their organization.

III. Understanding the Cost of Compliance

In order to effectively address the cost considerations of compliance, an organization must first have an accurate and comprehensive approach to understanding costs. One issue that frequently hinders such an understanding is the minimal level of experience of many security professionals in the financial aspects of business. An analysis performed solely by security personnel will frequently omit significant cost factors such as personnel costs. Organizations that wish to undertake such an approach should ensure that the team responsible for documenting the costs should include personnel with expertise in finance and human resources in addition to security personnel.

Types of Costs

There are three categories of expenses that need to be understood in order to effectively quantify the cost of compliance. These are

- **Operating expenses** – expenses for which the value is realized in the short-term – typically, a year or less. Examples of operating expenses include software maintenance fees, consumable supplies and annual subscriptions.
- **Personnel costs**. This includes salaries and wages. Most organizations utilize an annual loaded cost for personnel that equals approximately 2 times their annual salary. Personnel costs are critical to understanding the costs of processes that have been implemented for compliance purposes.
- **Capital investment**. These are expenditures in which value is derived by the organization over an extended period of time. For example, laptop computers may provide utility to an organization for three to five years.

The team should agree on the types of costs and how they are calculated, based on the organization's specific approach. In addition, the appropriate sources for each type of costs should be consulted. For example, the Purchasing department can usually provide details on items such as vendor maintenance contracts, the Human Resources department can provide loaded personnel costs, and the Finance department can provide details on capital investment costs.

Another area that should be considered is the time period that will be used for the cost analysis. It is generally easiest to understand costs as a yearly function, although some organizations may choose to break it down even further to quarterly or even monthly costs.

Documenting Costs

Once the categories of costs have been agreed upon and documented, the next step is to perform a detailed analysis of the organization's information ecosystem to identify and document all costs associated with compliance efforts. The most common approach to this is to have security personnel make a list of the various controls they know about and document the costs associated with them. Unfortunately, this approach is generally not the best one, as it tends to miss large areas of costs that traditional security personnel may not consider. For example, while expenses related to disaster recovery (DR) and business continuance (BC) may be incurred specifically due to requirements in regulations such as the U.S. Federal Financial Institutions Examination Council regulation, security personnel may not consider them since DR/BC solutions are frequently implemented by IT departments with minimal security involvement.

A more effective approach is to utilize an existing standards-based framework as a form of checklist to ensure that the costs for all security- and compliance-related controls are documented and analyzed. By utilizing an existing framework that incorporates all possible compliance controls, an organization can leverage the extensive work performed by industry and/or government organizations and not have to invest resources to create their own list. While a number of suitable frameworks are available, such as NIST 800-53 and ITIL, RSA recommends the ISO 27002 standard (formerly known as ISO 17799) as the most comprehensive and useful for this type of analysis. This view is shared by a number of industry analysts, such as The Burton Group in their report title *'Enterprise Security Control Standards: Which Ones and Where They Apply'*, dated October 1, 2007.

A common approach to the actual data collection and analysis effort is to utilize a spreadsheet tool to document costs. Utilizing ISO 27002, each type of control is documented in a separate row in the spreadsheet, with columns representing a functional grouping that utilizes or drives such controls, such as organizational units (e.g. division, agency, group), specific requirements (e.g. SOX, PCI, etc.) or specific types of information (e.g. credit card data, PII, PHI, etc.). The cost of a given type of control for the given grouping is documented in the intersecting cell, and the total costs are computed for each row and column using automated formulas. Note that computing the total cost of a given control should factor in all costs, including license and maintenance fees for a product, management costs, personnel time devoted to a process, server resources required to run software, etc. In many instances these costs may rely on costs computed for a given resource by another group within the company. For example, the cost of maintaining a Windows server to run a security tool may need to come from the IT department, the cost of network bandwidth utilized for backup may need to come from the networking group, etc.

It may also be worthwhile to document labor and non-labor costs separately. Since labor is generally the most expensive component, being able to understand labor costs separately may help point to areas where processes are inefficient.

In order to effectively address the cost considerations of compliance, an organization must first have an accurate and comprehensive approach to understanding costs.

Consider the following simple example:

	Division A	Division B	Corporate IT	Total
Monitoring	\$12,000	\$22,000	\$40,000	\$74,000
Authentication	\$20,000	\$0	\$50,000	\$70,000
Backup	\$60,000	\$45,000	\$60,000	\$165,000
Total	\$92,000	\$67,000	\$150,000	\$309,000

Detailed information on how each cost was computed should be documented, and an active link created between each cost cell and its associated information.

Once this exercise has been completed, the number computed in the lower right-hand corner of the spreadsheet represents the total spending by the organization on compliance. The spreadsheet should be reviewed by management and the executive/director staff to ensure a common understanding of the costs associated with compliance.

Another benefit of this approach is that it will help identify areas where inadequate controls have been implemented. If the control defined on a given row is viewed as a critical

requirement for one or more functional groupings and it shows little or no associated costs, it's immediately obvious that that area needs to be addressed.

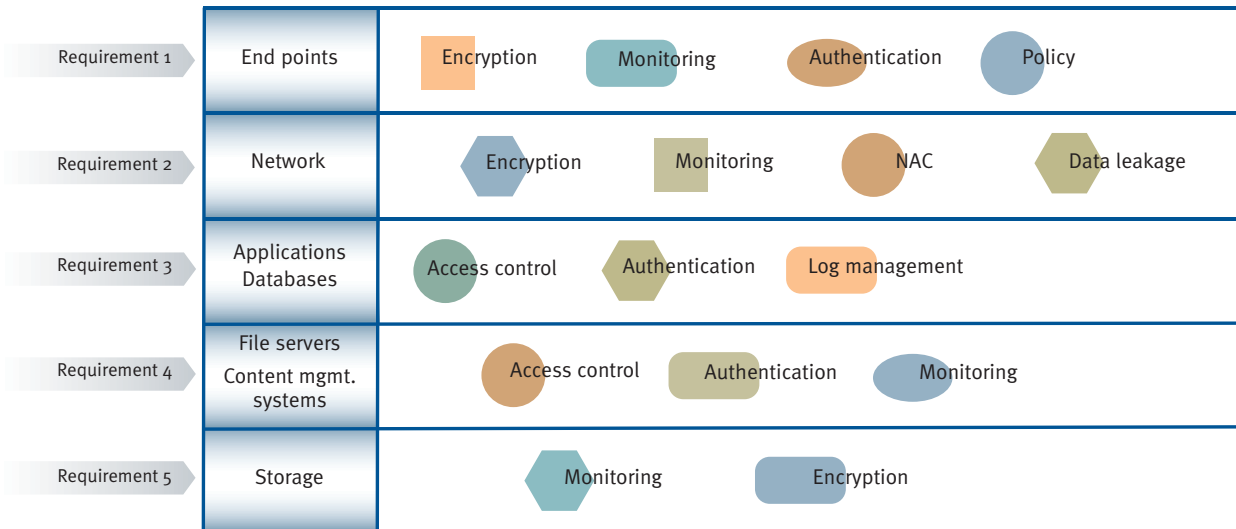
IV. Managing the Cost of Compliance

Once an organization has a comprehensive view of how much they are spending on compliance, the next step is to analyze the information to determine how costs can be reduced. The most obvious areas to start looking at are those controls that have the greatest expense associated with them across the organization. If the cost analysis shows a large number of controls with high costs across multiple functional groups, the organization may be able to significantly reduce costs through the use of a framework-based approach to implementing compliance-based security controls.

A Framework-based Approach

When implementing security and compliance solutions, most organizations have traditionally taken a project-based approach, treating each unique set of functional requirements as a unique project. This approach is typically augmented with the implementation of point solutions over time to address unique requirements as they arise. This results in a hodgepodge of different solutions, many of which perform related or even identical functions in support of different requirements. Figure 1 illustrates this approach.

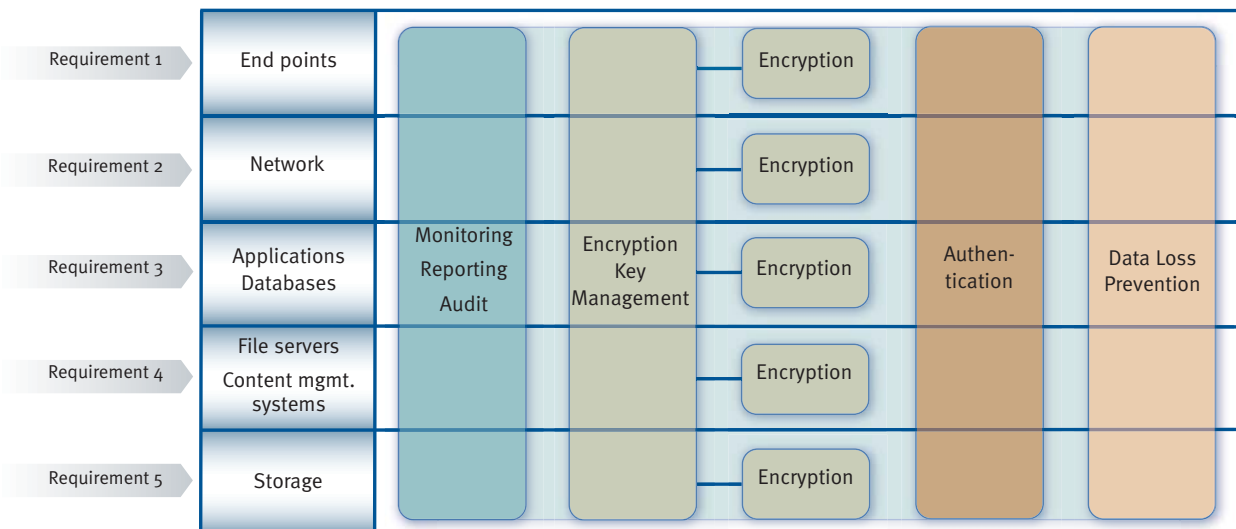
Figure 1. A typical hodgepodge of different point solutions



The impact of this approach shows up in the cost analysis as multiple high-expense cells in the same row, all addressing the same type of control requirements but in different functional areas.

A framework-based approach implies that, for a given type of control requirement, a single solution or limited set of solutions is implemented to address that requirement, regardless of the functional area in the organization that may drive that requirement. The result is a reduced number of discrete control solutions that still meet the organization's requirements but at a significantly reduced cost. Figure 2 illustrates this approach.

Figure 2. A framework-based approach



As with the cost analysis, leveraging a standard such as ISO 27002 can prove invaluable in implementing this type of framework-based approach. By utilizing the comprehensive list of controls defined in ISO 27002 in a framework-like manner, an organization can ensure that all critical controls are implemented utilizing a single common set of solutions that meet most if not all of the requirements from all functional groupings. The result can be a significant reduction in the number of controls in the organization, and hence a significant reduction in total costs. These savings have been documented by industry analysts such as Gartner in their report titled *'How to Implement a Risk-Oriented Approach to Compliance'*, dated August 22, 2006. According to Gartner, organizations that have taken this type of approach have been able to reduce their total number of controls by 30% to 70%.

While implementing an ISO 27002 framework may reduce costs and improve overall security, care must be taken to ensure that the solutions that are implemented in support of the framework can meet the organization's full range of requirements. For example, if an organization has multiple different monitoring requirements across different functional areas, care should be taken to ensure that the

RSA and EMC provide one of the widest ranges of solutions available to support customers in implementing an ISO 27002-based security and compliance framework. In order to assist customers in understanding how our solutions and capabilities map to the ISO 27002 framework, RSA has created the ISO 27002 Solutions Navigator, available on our web site at <http://www.rsa.com>. With this Navigator, customers can select specific ISO controls and view a list of solutions that can implement those controls, along with a mapping of those controls to various government and industry

framework monitoring solution that is implemented can meet all of these different requirements. If no single solution can meet all of an organization's monitoring requirements, multiple solutions may be required, possibly reducing the cost benefits of the framework approach.

The following factors should be carefully considered when selecting framework-based solutions:

- **Scalability.** Can the solution support the full number of objects (e.g., users, servers, databases, etc.) required by the organization across all functional areas? Can it do so with an adequate level of performance? Can it support the level of growth anticipated by the organization? If not, multiple instances of the solution may be required, increasing costs.
- **Flexibility.** Does the solution support a range of options in its functional area? For example, does an authentication solution support the various levels of authentication and form factors required within all functional groups? If not, multiple solutions may be required to implement a single control across all area of the organization, increasing costs.
- **Availability.** Does the solution provide or support methods to ensure high availability? When migrating from multiple disparate solutions to a single integrated one, a lack of high availability for that single solution can have a much broader impact across the organization.
- **Separation of Duties.** Does the solution provide the ability to partition management and operational capabilities across multiple functional areas within a single instance? For example, if different groups in the organization need to be able to manage their own encryption keys, can this be supported with a single instance of a key manager, or will multiple installations be required?
- **Integration.** Does the solution integrate with other components in the infrastructure out of the box, or will extensive customization be required? Lack of out-of-the-box integration may require customization or force the implementation of multiple solutions, increasing costs.

RSA and EMC provide one the widest ranges of framework-class solutions available in the industry, with customer-proven scalability, flexibility and availability options. These solutions cover an extensive range of the ISO 27002 controls, including:

- Data security, such as encryption, encryption key management and data loss prevention
- Authentication and authorization, such as multi-factor authentication, web-based single sign-on, and consumer protection
- Security information and event management, including log collection and management and real-time event analysis
- Backup, recovery and archiving tools
- Disaster recovery/business continuance solutions

In addition, RSA and EMC have invested heavily in the integration of their solutions, ensuring that multiple solutions can work together right out of the box.

- **Multifunction Solutions.** Does the solution support the implementation of multiple controls in a single package? For example, a single tool that can collect, store and automatically lifecycle manage event logs for reporting and forensics purposes as well as perform real-time analysis of those logs for alerting would be less expensive than two tools to perform both of these functions.

By selecting and implementing appropriate solutions across the organization in a framework-based approach, organizations can reduce the number of discrete controls in their environment, significantly reducing costs. It should also be noted that this approach does not necessarily mandate that an organization replace all of their existing controls with new ones; in many instances, an organization may have an existing solution in place that can be expanded to cover other functional areas, eliminating the need to acquire or implement new controls.

Sustainable Compliance

One additional advantage to this framework-based approach is that, if implemented correctly, it can prepare an organization to address new and changed requirements as required. This is particularly true if ISO 27002 is used as the base framework, due to the fact that the International Organization for Standardization (ISO), (which is responsible for ISO 27002) reviewed hundreds of different government regulations worldwide and incorporated a common set of controls in 27002 that allow it to meet the majority of those regulations. If an organization has implemented a comprehensive ISO 27002-based framework of control solutions, the probability that the controls required to meet a new or modified set of requirements are already in place is very high. As a result compliance becomes an exercise in simply expanding the existing controls to cover the areas addressed in the new or modified requirements, as opposed to starting a new project and acquiring and implementing new controls.

This advantage also exists where the infrastructure itself changes but compliance requirements do not. For example, if a new application and server are installed to processes information covered by an existing set of requirements, the existing framework controls can be easily expanded to cover the new components without having to purchase or create new ones.

The cost savings associated with this future-proofing continue to accrue far beyond what was originally gained.

Other Measures

While implementing a framework-based approach to compliance can potentially provide the most significant cost savings, there are other approaches that can help further reduce costs. These are discussed below.

Automation

When performing a cost analysis, tracking the labor related with the various controls separately can provide valuable insight into areas where manual processes result in significant costs to the organization. One way an organization can reduce labor costs is to automate these manual processes with tools. Modern security software and compliance tools can replace a significant number of processes that many organizations have traditionally accomplished manually. For example, responding to audits has typically been a very manual process, requiring significant IT resources to collect and correlate information

RSA and EMC provide a wide range of solutions that support extensive automation of what have traditionally been manual processes. This includes areas such as monitoring, auditing and reporting, data loss prevention and strong authentication for user self-help capabilities.

and create reports. Modern security information and event management (SIEM) tools can replace these manual processes with a few mouse clicks, reducing or even entirely eliminating manual effort.

Vendor Support

Traditionally, as new components such as servers, applications, databases, etc. are acquired and installed, security personnel would ‘bolt on’ the security capabilities necessary for compliance. For example, if an organization wanted to encrypt their backup tapes on a FibreChannel Storage Area Network (SAN), they would have to purchase an appliance to add inline on the SAN, or purchase new encrypting tape drives. This lack of integrated security functionality results in increased costs as more components must be added and managed.

To reduce the added cost in the infrastructure necessary for compliance, customers should mandate that required security functionality be integrated into any products they acquire. For example, any products that ‘touch’ sensitive information should incorporate encryption, and all products should support some form of event logging to allow monitoring from a centralized tool.

In addition to integration of security functionality, customers should mandate that any integrated functionality in products they acquire from one vendor should integrate with external security and compliance solutions from others. For example, encryption solutions should support external lifecycle management of encryption keys by a centralized key manager, event logging should be manageable by a centralized SIEM solution, and user authentication should support external multi-factor authentication capabilities.

Infrastructure Consolidation

In many instances, the reason that multiple solutions addressing a single type of control requirement have been implemented across an organization is that different IT infrastructure components have been implemented and managed separately in different functional areas. Even though implementing a framework-based solution may be able to handle common requirements across all of these areas, significant cost savings may be realized by consolidating a large number of disparate operations into fewer centralized ones. Consider storage – while SIEM tools can monitor a wide range of disparate storage-related solutions spread out across an organization, the process of monitoring will ultimately be much simpler, and hence much cheaper, if the storage were consolidated and managed in a central location. One of the most significant areas of cost savings in this scenario is the ability to eliminate a lot of potentially redundant solutions, reducing the number of components that need to be monitored.

RSA and EMC have implemented extensive programs to ensure that our solutions integrate the latest advanced security functionality directly into our products. For example, EMC PowerPath® multi-pathing software for EMC and third-party storage environments directly integrates RSA’s advanced encryption capabilities, which in turn support the use of RSA Key Manager for centralized key management.

RSA and EMC have also undertaken extensive integration efforts with our partners. RSA Key Manager supports centralized manage of keys for products from EMC, Cisco, Brocade, Oracle and others, while our enVision solution can collect and analyze event logs from over 130 third-party products.

V. Summary

While every organization recognizes the importance of complying with all applicable internal and external security requirements, many are forced by economic reality to focus on reducing the overall amount of resources they can devote to their compliance efforts. While drastic cost-cutting might seem like the only possible solution, RSA believes that a structured approach to understanding and minimizing costs can result in significant saving while at the same time maintaining or even improving overall compliance. Once an organization has a comprehensive understanding of exactly where the costs are across all functional areas, they can then begin to implement a set of framework-based solutions that can reduce or eliminate

redundant controls, significantly reducing costs to the organization. Additional approaches that can further reduce costs include automation of manual processes, mandating vendor support for compliance efforts, and consolidating their overall infrastructure.

References

For more details on the RSA and EMC solutions mentioned in this white paper, please refer to our web sites at <http://www.rsa.com> and <http://www.emc.com>. More information regarding RSA solutions for compliance may be found at www.rsa.com/compliance.

EMC is the industry leader in solutions to assist customers in consolidating assets that impact their critical information, such as storage, backup, archiving and disaster recovery. Integration of these solutions with RSA's advanced security management functionality in areas such as key management, security and compliance monitoring, and data loss prevention ensures that the a broad range of compliance requirements can be met with the least amount of resources, thereby reducing costs.

About RSA

RSA, The Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

About the Author

John McDonald is the team leader of RSA's Security Evangelist team, which is responsible for working with customers to deliver the EMC/RSA message and strategy. He has over 25 years experience in the security industry, and has been actively involved with security at EMC since he joined the company over 6 years ago. Before EMC he worked with several consulting companies performing security audits and security infrastructure design for numerous customers, including several Fortune 500 ones. John is a CISSP.



RSA, the RSA logo and RSA Security are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC and PowerPath are registered trademarks of EMC Corporation. All other products or services mentioned are trademarks of their respective owners. ©2008 RSA Security Inc. All rights reserved.

CCC WP 0708



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC