

RSA Executive Overview

## Information Risk Management for the Public Sector

# Information-centric Security

As the single most important asset in our economy, information has the potential to help you meet your mission, to protect you or to get you in trouble. Focusing on information itself clarifies operational context, and following its path across your IT infrastructure reveals where it is potentially vulnerable.

---

## The Growing Challenge

---

Over the past few years we have all become increasingly aware of data security risks in the public sector. From hackers who broke into the U.S. Department of Agriculture in June 2006, to a U.K. data breach in November of 2007, concern that government organizations need to strengthen their data security operations is mounting globally.

In the case of the U.S. Department of Agriculture, hackers gained access to over 25,000 agency employee and contractor names, Social Security numbers and photos. In the U.K., in what appears to be the largest single breach to date, two computer discs with the personal details of all families in the U.K. with a child under age 16 were lost.

As noted by the BBC News on November 20, 2007,

*“The Child Benefit data on them includes name, address, date of birth, National Insurance number and, where relevant, bank details of 25 million people. Chancellor Alistair Darling said there was no evidence the data had gone to criminals ... The Conservatives described the incident as a ‘catastrophic’ failure... Mr. Darling apologized for what he described as an ‘extremely serious failure on the part of HMRC to protect sensitive personal data entrusted to it in breach of its own guidelines’”.*

The problem, whether in the U.S., U.K., Brazil or Singapore is that the classic approach to information security fails to address the modern “data-centric” threat environment. This makes the role of the government CISO increasingly difficult. Look at what compliance regulations might be on a federal or state CISO’s plate, recognizing for the moment that while the names and specifics may vary at the federal, state, county and municipal levels, the challenges are similarly daunting.

**What actions are you taking to assure cyber security?**

---

## The Effects of U.S. Federal Government Mandates

---

### FISMA

Assume for the moment that an agency is in good standing under the Federal Information Security Management Act; meaning that system boundaries and FIPS-199 categorizations are complete and accurate, systems are documented, risk assessments are current, security controls are in place – certified, accredited and monitored. The ongoing governance of this program is no small task. There’s a ‘FISMA-effect’ every time a new system is brought online or upgraded. New risk assessments bring to light varying conditions, resulting in recommended changes to security and control systems.

### OMB 6-16 and 7-16

In addition to statute and regulatory requirements, The Office of Management and Budget has issued recent guidance focused predominantly on information protection. While some of the requirements are straightforward (such as two-factor authentication for remote access), and some requirements are largely a restatement of FISMA, others – such as the review and classification of data holdings, the reduction of Social Security numbers, and publication and enforcement of detailed breach notification policies – may require entirely new internal initiatives.

### Comprehensive National Cybersecurity Initiative / CNCI

Established in January 2008 by Homeland Security Presidential Directive 23/National Security Presidential Directive 54, the U.S. Federal Government’s Cyber Initiative is a multi-agency, multi-year plan that is initially focused on 12 initiatives for securing the federal government’s and defense industrial base’s cyber networks and information systems. Most of the CNCI is currently classified.

As U.S. federal agencies and the defense industrial base implement requirements related to the Cyber Initiative, there is a strong focus on access controls, information protection, information integrity, product assurance and reducing the number of external Internet connections within government agencies (via the Trusted Internet Connection initiative). The CNCI is also spurring more investment in, and focus on, infrastructure security awareness capabilities for use throughout federal civilian agencies with programs such as Einstein.

---

## Taking a Global Perspective

---

While information security is acknowledged as an issue on a global basis, regional and local approaches can vary greatly. There are widely differing policies and enforcement mechanisms in the Asia-Pacific region, including class actions, mediation and public apologies, in contrast to the long established civil and criminal sanctions present in Europe and North America.

In the Asia-Pacific region, attacks on the confidentiality, integrity and availability of data and systems are significant. Threats to critical infrastructure and national interests arising from criminal activity on the Internet are of growing concern. The Asia-Pacific Economic Cooperation (APEC) Privacy Framework works to prevent and combat the harm incurred to governments and individuals in member economies while avoiding the creation of unnecessary barriers to information flows.

Moreover, the EU Data Protection Directive mandates that governments and corporations protect the privacy of citizens as information is stored and transferred among member countries and between organizations. Member states are charged with maintaining a supervisory authority to ensure that country-specific mandates around personal information privacy are upheld. To add more complexity to the matter, authorities in member states must ensure that transfers of private data to non-EU member states are adequately protected. No small task, indeed.

Finally, the Organization for Economic Co-operation and Development (OECD) states that “Security must become an integral part of the daily routine of individuals, businesses and governments in their use of [technology] and conduct of online activities”. The OECD’s Working Party on Information Security and Privacy (WPISP) aims to help OECD member and non-member countries share policies and best practices to promote a Culture of Security through the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (“OECD Security Guidelines”).

On a global basis, governments are addressing the problems and challenges around data security, and are drawing on international instruments such as the OECD Guidelines, the Council of Europe Convention, the UN Guidelines, the EU Directive and the APEC Framework. There’s still a long way to go, but processes are in place and progress is being made at many different levels.

---

## The Rising Tide

---

Amidst all of these requirements, there is still the day-to-day job of staving off intruders – tens of thousands of attacks daily, viruses and Trojans, and the very real prospect of data loss – of both Personally Identifiable Information (PII) and sensitive, mission-critical data that might apply to public safety, national security or operational readiness.

Despite the rising tide, resources to stem it remain finite. Because of this, EMC and RSA, the Security Division of EMC, work with key systems integrator partners and directly with public sector agencies to enable customers to protect information using a risk-based approach to security. Recognizing that information assurance relies on product assurance, EMC engages in robust product security initiatives – building security into our products – which allows public sector agencies to do more with less.

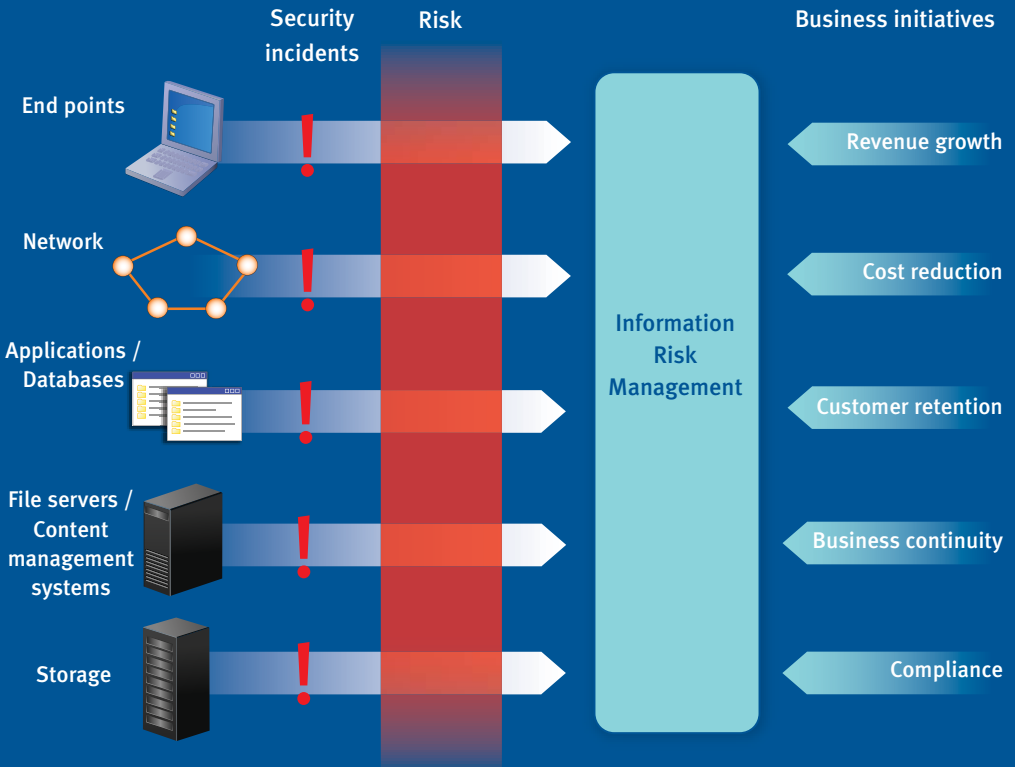
In today's era of relentless cyber-crime, it is more important than ever to have a layered information risk management strategy aimed at the most pressing risks to your information and assets, and to have a trusted and reliable partner with a wide range of information-centric security solutions and capabilities.

**Do you know where all the  
classified information in your  
agency is stored?**



*“For us to effectively implement controls into the enterprise, my theory is that we have to have a risk-based approach, because we’re fundamentally poor. I cannot spend all the money, even if I wanted to. So we have to take the most effective approach at identifying those potential risks to the business and protecting those things that need protecting.”*

Roland Cloutier  
Vice President, Chief Security Officer  
EMC Corporation



Information risk management reveals where to invest, why to invest, and how security investments map to critical business objectives.

---

## Information Risk Management.

---

Assessing information risks puts security into context clarifying and aligning organizational mission with IT security priorities. RSA’s approach to managing information risk in an IT setting is distinguished by three characteristics:

- 1. Information-centric.** As the single most important asset in our economy information has the potential to help you meet your mission, to protect you, or to get you in trouble. Focusing on information itself clarifies operational context, and following its path across your IT infrastructure reveals where it is potentially vulnerable.
- 2. Risk-based.** Using risk as a lens for your security investment decisions ensures that the most significant challenges are addressed first.
- 3. Repeatable.** Emphasizing the implementation of processes and solutions based on standards and best practices that can be leveraged across multiple security and compliance initiatives, in order to save time, money and effort.

Information risk management reveals where to invest, why to invest, and how security investments map to mission-critical operations.

In government, critical initiatives may include meeting compliance requirements, safeguarding national security or even maintaining a public-facing service such as a citizen portal. Whatever the top initiatives, information needs to be the primary focus – what are the most sensitive information assets that are critical to the organization? Where and how do they travel across the IT infrastructure (endpoints, networks, applications and databases, file systems and content management repositories, and storage systems)? As they travel, what risks are they exposed to? What security events might take place? How likely are they to occur, and what are the consequence if they do?

**What are you doing to prevent  
“cyber espionage”?**

Whether your organization deals with citizen rights and welfare, government operations, public resource management, or national safety and defense, you have critical information that needs to be protected from loss, and misuse.

**Managing information risk is a four step process.**

1. **Discover and classify** to find all the sources of sensitive information across the organization and categorize its sensitivity
2. **Build policy** to address how information should be protected. Policies should consider the data objects themselves, who can access the data, and how the infrastructure that stores and processes the information needs to be secured.
3. **Deploy security controls** to enforce the policy. This control framework ideally should be based on established security best practices or standards like NIST SP 800-53 series, ensuring that it is broadly applicable and effective in addressing most security challenges. The range of controls will be wide, but data controls and access controls should be applied
4. **Monitor the effectiveness of controls**, audit and document compliance with policy.

**How do you track access to systems and data?**

---

## Where EMC and RSA can help in each of these areas

---

### Discover and Classify

The explosion of data captured and stored by government agencies presents an information management challenge. Information that is unmanaged cannot be effectively secured. Agencies need to first discover all the sources of sensitive information across the infrastructure.

To aid this process, RSA offers information classification and discovery services, as well as automated tools that can discover infrastructure components and map application dependencies and continually search endpoints and dead center repositories for targeted content.

**RSA RiskAdvisor** grants agencies visibility into the information risk that they face by locating sensitive unprotected information. The service offers remediation recommendations based on information risk priorities.

**EMC Smarts® ADM** discovers and builds a model of all the applications in an IT environment, showing the interdependencies and connections among applications. For example, this tool provides a record of all applications that might have access to PII.

**RSA Storage Security Assessment Service** evaluates the security posture of networked storage deployment (SANs, NAS & CAS) in accordance with approved practices and proposes improvements to critical components.

### Data Controls

Data controls protect sensitive data, structured and unstructured, wherever it resides.

The **RSA Data Loss Prevention (DLP) Suite** searches stores of unstructured data locating specific bits which match customer-defined criteria such as Social Security numbers or credit card numbers. It enables agencies to define and manage policy centrally and prevents unauthorized outflow of highly sensitive data from the network and end points. The RSA DLP Suite addresses content in use (on end points), content in motion (on the network and on applications such as e-mail and web portals) and content at rest (in databases, file servers and storage).

The **RSA Encryption Suite** encrypts sensitive data at multiple points in the infrastructure and manages the lifecycle of encryption keys across the enterprise. RSA offers encryption solutions for applications, file servers and storage, and we partner for solutions on endpoints, databases, and on the network.

**RSA® Key Manager** alleviates the formidable challenges of key management by simplifying and centralizing the management of keys.

**RSA BSAFE®** encryption toolkits provide a complete portfolio of cryptography solutions for developers to meet the security goals of their applications. These tools allow developers to meet the stringent FIPS 140 and Suite B requirements for offering products to U.S. government agencies.

**EMC Documentum's Information Rights Management Suite** enables secure document sharing across an extended enterprise. It provides persistent protection, allowing users to dynamically control access and use of documents and emails inside and outside the organization throughout their entire lifecycle.

**EMC Certified Data Erasure** permanently erases data from disk, up to D.O.D. specifications, as devices are retired or re-purposed.

### **Access Controls**

Access controls enable secure access to information infrastructure and secure transactions for employees, citizens and contractors. RSA's access controls support an essential process we call Identity Assurance.

Identity Assurance enables organizations to create new information-flow models that take advantage of a worldwide community. With identity assurance, employees, contractors and citizens freely and securely interact with systems, applications, and information, opening the door for new ways to deliver services, satisfy customers, and control costs.

**Can your contractors and partners  
access critical information?**



*“The biggest hindrances to greater encryption are cost and complexity – and much of the operational complexity comes from complications associated with key management. Putting in place streamlined key management processes can reduce apprehension about increased encryption deployment, and thus improve the business case for better data protection.”*

Forrester Consulting  
The State of Data Security in North America  
August 2007

The four components of Identity Assurance are: credential management, authentication, contextual authorization and intelligence.

**Credential management** defines identity policy and manages the lifecycle of credentials used for authentication.

**RSA® Authentication Manager** software is the management component of the RSA SecurID® solution, used to verify authentication requests and centrally administer authentication policies for enterprise networks.

**Authentication** validates the identity of internal and external users to systems and resources via hosted, appliance, or on-premise applications.

RSA SecurID authentication, the market-leading strong authentication solution, uses hardware and software-based credentials (tokens) to validate the identity of users. SecurID technology is interoperable with more than 300 products from more than 200 vendors, including most leading VPN providers.

**RSA® Digital Certificate Solutions** offer interoperable modules for managing digital certificates and creating an environment for authenticated, private and legally binding electronic communications and transactions.

**RSA® Adaptive Authentication** provides flexible cost-effective protection for the entire end user base. Risk-based authentication operates behind-the-scenes and works by positively identifying a user and performing a comprehensive risk assessment of any given activity

**RSA® Identity Verification** verifies user identities in real-time and helps prevent the risk of fraud and identity theft. Utilizing knowledge-based authentication (KBA), this tool presents a user with top of mind questions utilizing relevant facts on the individual obtained by scanning dozens of public record databases. It delivers a confirmation of identity within seconds, without requiring a prior relationship with the user.

**Contextual authorization** manages access and federates identities, enforcing policy across web resources, portals, and applications.

**RSA® Access Manager** leverages trusted identities to control access to web applications. It manages large numbers of users while enforcing a centralized security policy that protects resources from unauthorized access. Single sign-on access to multiple web-based resources makes legitimate users more productive.

**RSA® Federated Identity Manager** securely exchanges user identities across organizational boundaries and with citizens and contractors. It allows organizations to collaborate while maintaining consistent and centralized control over the policies associated with users and applications.

**Identity and activity intelligence** mitigates identity misuse and abuse and collects intelligence on emerging threats.

The **RSA® FraudAction<sup>SM</sup>** service is an anti-phishing/anti-pharming and anti-Trojan service that combats cyber attacks against government resources with 24x7 monitoring and detection, real-time alerts and reporting, site blocking, forensics, countermeasures, and site shutdown. The FraudAction service is supported by RSA's exclusive Anti-Fraud Command Center (AFCC), which has been responsible for shutting down over 90,000 fraudulent sites and reducing the average lifespan of an attack from 115 hours to just 5 hours.

### **Monitor, Report and Audit**

Finally, government agencies need to ensure that their security controls are performing. monitoring, reporting and auditing allows organizations to detect security anomalies and potential threats and to validate compliance with security policy and regulations. Security information and event management (SIEM) tools provide this capability helping to promote a more strategic view of organizational data.

**Can you seamlessly and securely share information across government agencies?**

The RSA enVision® platform captures and stores up to hundreds of thousands of data events per second, providing an infrastructure-wide view of activity from any number of sources, including perimeter and network devices, operating systems and even proprietary applications and transforms this information into valuable intelligence. From a security operations perspective, this information can be used in real-time to alert security administrators of policy violations and for forensic analysis of security policy effectiveness. From a compliance perspective, this information can be used to produce reports outlining compliance with regulations across industries and government entities. Move from an activity monitoring model to an exception monitoring model.

A key component of RSA enVision technology is its ability to store and retain the vast amounts of security data that is collected. To this end, RSA enVision is integrated with EMC storage systems to cost-effectively store and manage this information throughout its lifecycle.

---

## **Realizing the Benefits of an Information Risk Management Program**

---

Many senior security government officials have found that implementing a risk-based security program not only ensures visibility of all the necessary touch points, but also prioritizes projects with the greatest benefit to the overall security posture. Subsequently, security managers are able to present their compliance efforts within the context of these programs, assuring inspectors, regulators and agency officials that appropriate measures are being taken and critical information security needs are being met with a feasible, strategic plan.

RSA continually strives to partner with our security colleagues in the government and public sector to assist in meeting these challenges.



With EMC and RSA's Common Criteria certified products, your organization can achieve compliance with various global Public Sector security procurement mandates such as the National Information Assurance Acquisition Policy (NSTISSP 11) in the USA, and fast accreditation of secure IT products to manage security throughout your information lifecycles. Certification enables you to achieve:

- Compliance: Achieve government-mandated Common Criteria and public/private sector ISO 15408 requirements for secure products.
- Assurance: Rely on pre-validated products to build assurance for your information infrastructure.
- Efficient procurement: Experience faster buying and accreditation cycles.

Common Criteria-conforming EMC Products	Evaluated Assurance Level
EMC Documentum® Content Server V5.3 and EMC Documentum Administrator V5.3	EAL 2
RSA® Certificate Manager V6.7	EAL 4+
VMware® ESX Server 2.5.0 and VirtualCenter 1.2.0	EAL 2
EMC ControlCenter v5.2 Service Pack 5	EAL 2+
EMC SMARTS® Service Assurance Management Suite and Internet Protocol Management Suite 6.5.1 w/ Storage Insight for Availability 1.0	EAL 2
EMC SMARTS Service Assurance Management Suite 7.1, SAM Adapters 1.1 and Internet Protocol Management Suite 7.0.2 w/ Storage Insight for Availability 2.0.1	EAL 2
EMC CLARiiON® FLARE v3.24 with Navisphere version 6.24 running on CX3 series storage systems	EAL 2+
EMC Celerra® Network Server v5.5	EAL 2+
EMC Symmetrix® Access Controls, Enginuity version 5771 with EMC Solutions Enabler v6.3	EAL 2+
EMC Disk Library – Release 3.1	EAL 2+

©2008 RSA Security Inc. All rights reserved.

RSA, the RSA logo, SecurID, BSAFE, FraudAction and enVision are registered trademarks or trademarks of RSA Security Inc. in the U.S. and/or other countries. EMC, Documentum, VMware, SMARTS, CLARiiON, Celerra, and Symmetrix are registered trademarks of EMC Corporation. All other trademarks mentioned herein are the property of their respective owners.

## 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](http://www.RSA.com) and [www.EMC.com](http://www.EMC.com).



RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)

The Security Division of EMC

**EMC<sup>2</sup>**  
where information lives<sup>®</sup>

GOV OV 0109