



The Security Division of EMC



RSA Solution Brief

# RSA Solutions for Mitigating Insider Risk

# Can you name five risks that employees pose to your business information and IT systems?

You probably can; but which occurred to you first? Did you think of deliberate acts such as information sold for financial gain; data theft by a contractor leaving your employ; a system hack or virus attack by a disgruntled employee? Or did you think of a lost laptop; a file saved on an unsecured shared area; or a virus unintentionally downloaded from a legitimate website?

The fact is that every organization is vulnerable to a wide variety of risk from insiders, only a small proportion of which is unambiguously down to deliberate attack, theft or fraud by malicious, disgruntled or compromised individuals. 'Insider threat' is only one type of 'insider risk'; most insider risk is the result of non-malicious, non-deliberate activity. IDC confirmed this in a survey of 400 CXOs from the U.S., UK, France and Germany: only 19% of respondents believed that incidents arising from internal breaches were predominantly deliberate.

Given the vast scope for employees to breach security unintentionally, and the never-ending media stories of CDs lost in the mail, laptops left on trains and personal data exposed on websites, one would think that insider risk would be an area of specific focus for most organizations. Yet more than half of the respondents had no security budget specifically allocated to addressing insider risk.

Why this dichotomy?

---

## A Question of Trust?

---

Part of the reason might be that unintentional breaches of security and accidental data loss are an inevitable byproduct of the need to trust employees. Every organization needs to give its permanent, contract, and temporary staff access to the systems and information that let them do their jobs effectively; and mistakes will be made. Employers are understandably wary of damaging this relationship of trust, and they may feel that preventing carelessness and error would require restrictive security measures that would compromise both employee morale and productivity.

But this is simply not the case. With the right approach, much insider risk is readily controllable – without inconveniencing employees or compromising operational effectiveness. And it's an area that you can't afford to ignore, as business becomes ever more reliant on IT to connect an increasingly dispersed and varied workforce sharing information more widely and easily than ever before.

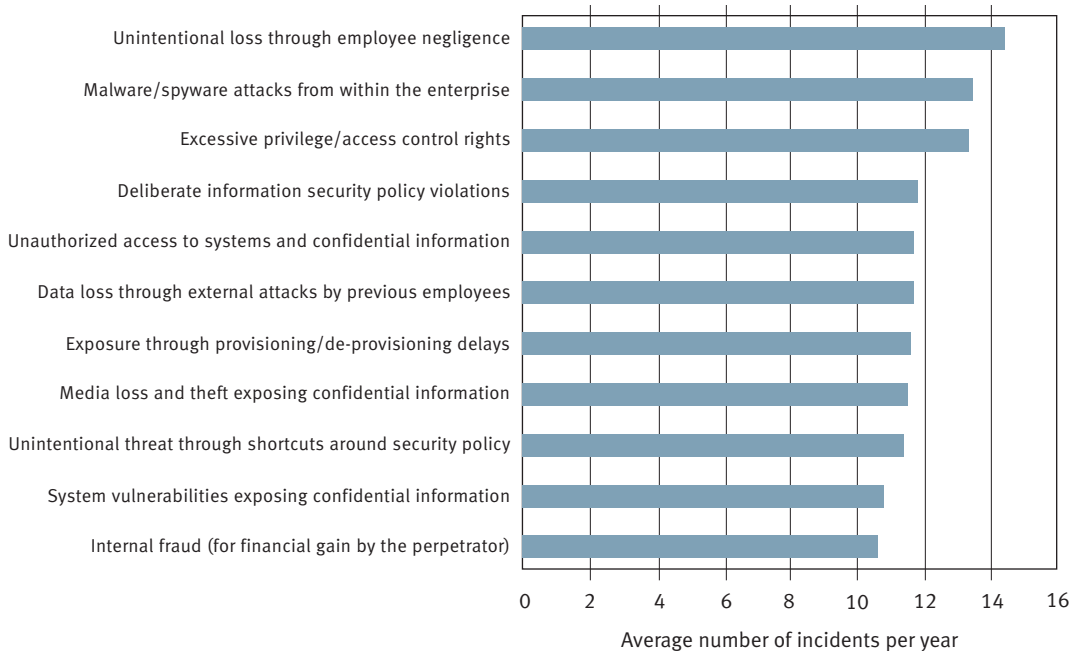
Addressing insider risk is the responsible thing to do and does not have to pose a challenge to employee trust. Failure to act, on the other hand, can cause far-reaching damage to your organization's reputation and market standing, not to mention the financial cost of investigation, remediation, and the possibility of fines for regulatory non-compliance.

**Insider risk arises from both intentional and unintentional behavior.**

- An America Online employee used a colleague's identity to obtain customer records, then sold 92 million e-mail addresses to spammers
- Ponemon Institute reported that 88% of data breaches were caused by simple negligence on the part of employees (*2008 Annual Study: Cost of a Data Breach*, February 2009)

### Average profile of internal security incidents

A survey of 400 CXOs by the IDC showed that, on average, organizations suffer this breakdown of internally caused incidents per year.



### Where to Start?

An ad-hoc approach – reacting to internal incidents as they occur, with point solutions – is neither cost-efficient nor effective in preventing future incidents. There are just too many ways for errors or carelessness to surface. Responding to a lost laptop with laptop encryption doesn't help when a CD or USB stick goes missing. Implementing better email security doesn't address file-sharing through IM clients. Forcing people to change passwords doesn't prevent them from writing them down.

The only effective, and cost-efficient, way to take insider risk seriously is to take an integrated and wide-ranging approach: to employ a risk management framework, backed by appropriate solutions, that lets you:

- Discover and quantify all areas of insider risk, so that you understand where to direct your security investments
- Create a prioritized roadmap of best practices for addressing insider risk
- Implement and enforce the roadmap with appropriate controls
- Monitor insider risk (employee behavior and incidents)
- Analyze and report on incidents and your responses to them, so as to identify areas for continuing improvement



---

## RSA's Approach

---

RSA has helped thousands of organizations take this approach to risk management. We won't talk about applying technology to your challenges until we've helped you understand your risk environment and developed a comprehensive risk management program that maximizes the effect of your security budget. When we do recommend specific solutions, it will be within the context of the framework developed for you, and they will be solutions that work together in an integrated way.

### Discover

In our experience, the number one challenge in tackling insider risk is lack of visibility of, and intelligence about, the risk landscape, so that's where we start. After all:

- How can you prevent loss, theft, or inappropriate transmission of sensitive information if you can't identify:

- What sensitive data you hold
- Where it resides and how it travels
- When its movement is insecure
- Who has access to it

- How can you control access to systems or information if you can't:

- Identify users' roles, especially those with access to high volumes of sensitive information
- Know when their responsibilities change or they're due to leave
- Recognize anomalous user behavior

RSA can help you gain a much better understanding of your internal risk exposure, including what sensitive data – intellectual property, confidential business information, customer data, personally identifiable information – you have throughout your infrastructure, from data center to endpoints.

### Enforce

Once you understand your risk landscape, you can direct your security investments to start mitigating your risks in order of priority.

We'll help you assess and develop your security policies in the context of a comprehensive risk management program and roadmap. You'll be able to implement a framework of appropriate technology controls to enforce your security policies, including data controls to minimize data loss, and access controls to assure the identity of all users and restrict their privileges to those needed for their current roles. You'll be able to monitor and track behavioral data for all users and devices, and be alerted to anomalous behavior for rule-based response or human escalation.

**RSA has unrivalled capabilities in securing identities, information and infrastructure.**

- Data classification and discovery
- Data loss prevention
- Encryption and key management
- Multi-factor and risk based authentication
- Role-based access control
- Behavior and transaction analytics
- Anomaly detection
- Log management
- Auditing
- Incident analysis
- Reporting

## Monitor and Report

Finally, RSA solutions can help you to audit and analyze security incidents and user behavior across your enterprise. You'll be able to spot developments that must be responded to, such as changes in user access patterns or types of security incident; identify and justify any required changes in investment; and generate reports for business and compliance purposes.

---

## RSA's Solutions for Mitigating Insider Risk

---

We've developed a comprehensive range of services and technology solutions to support our framework approach to mitigating insider risk. These work together to give you defense-in-depth against the variety of risks, both intentional and unintentional, that your employees – and, for that matter, outsiders as well – pose to your systems and information.

### RSA Professional Services

The RSA Professional Services team will help you discover and quantify your insider risk and create a prioritized roadmap of best practices for addressing them. We'll identify sensitive information across your network infrastructure, from data center to endpoints, and identify vulnerabilities in data protection. We'll assess your existing security policies, and help you update them or design new ones to reflect your risk and regulatory landscapes and current best practice. We'll work with you to develop a comprehensive risk management program, and design and implement an appropriate framework of technology controls to enforce your policies. RSA Professional Services include:

- RSA Information Risk Assessment service
- RSA DLP RiskAdvisor service
- RSA Information Security Policy Development Service

### RSA® Data Loss Prevention Suite

Our DLP capabilities start with Professional Services (see above) to discover data at risk, devise policies to protect it and design appropriate controls to enforce policies. We have a full range of DLP solutions to monitor and control data and its movements in the data center, across the network and on endpoints. The RSA® Data Loss Prevention Suite includes:

- RSA DLP RiskAdvisor service
- RSA DLP Datacenter
- RSA DLP Network
- RSA DLP Endpoint

### RSA Encryption and Key Management Suite

As an integral part of our framework of data controls to protect sensitive information, we offer a suite of data encryption and centralized encryption key management solutions, including:

- RSA® Key Manager with Application Encryption
- RSA® Key Manager for the Datacenter
- RSA BSAFE® encryption

Defense-in-depth against the variety of risks, both intentional and unintentional, that your employees – and, for that matter, outsiders as well – pose to your systems and information



### RSA Identity Protection and Verification Suite

These solutions use fraud trends, intelligence, forensics, modeling, transaction monitoring and multi-factor risk-based authentication to reduce the risks arising out of remote transactions. They include:

- RSA FraudAction<sup>SM</sup> service
- RSA<sup>®</sup> Transaction Monitoring
- RSA<sup>®</sup> Adaptive Authentication
- RSA<sup>®</sup> Identity Verification

### RSA Authentication

However your users are accessing your systems, we've got strong authentication solutions to meet all their requirements, without compromising user convenience or security. This means you can apply strong authentication to all users, not just those accessing systems remotely. Our authentication solutions include:

- RSA SecurID<sup>®</sup> authentication
- RSA<sup>®</sup> Adaptive Authentication
- RSA<sup>®</sup> Identity Verification

### RSA<sup>®</sup> Access Manager

Easily manage large numbers of users accessing web applications in intranets, extranets, portals and exchange infrastructures. Employees can do their jobs more easily with secure single sign-on, while you enjoy centralized control of access policies.

### RSA enVision<sup>®</sup> Platform

This security information and event management platform automatically collects, manages and analyzes logs from across your infrastructure, enabling you to monitor all systems; identify and keep a record of security events and information access; carry out forensic analysis and audits; and generate reports at a variety of levels of detail for business and compliance purposes.

### EMC Solutions

EMC has a range of server configuration and management solutions, network configuration and management solutions, and IT operations management solutions that help you to monitor and track changes on your infrastructure to ensure that policy is followed and events escalated for remediation if necessary.

#### Choosing RSA to take control of insider risk is a smart choice.

- Unrivalled expertise in securing identities, information and infrastructure
- Deep understanding of the nature and challenges of insider risk
- Comprehensive framework-based approach
- Award-winning security products and services
- Strong relationships with partners, especially our parent organization EMC



We work with you to develop a comprehensive risk management program, and design and implement an appropriate framework of technology controls to enforce your policies.

## RSA is your trusted partner

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, 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, LogSmart and *All the Data* are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC. Windows is a registered trademark of Microsoft Corporation in the U.S. and/or other countries. All other products or services mentioned are trademarks of their respective companies.

IRSK SB 0709



The Security Division of EMC

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