



The Security Division of EMC

White paper

An Information Risk Management Approach to Fighting Fraud



A Holistic Approach

RSA, the Security Division of EMC, has long been synonymous with the ability to fight fraud in the online banking and e-commerce channels. Increasingly, however, those responsible for fraud prevention within large organizations are looking for ways to address the risk of fraud more holistically within their businesses.

RSA has developed an information risk management strategy, which can be used as a tool to help address fraud more broadly. In this white paper we will explore how information risk management can be used in this context.

We will review some of the key trends that our Anti-Fraud Command Center (AFCC) is seeing, and how these trends are starting to affect organizations beyond the financial services sector. We'll then clarify exactly how and where RSA can help. Clearly there are all too many ways in which criminals can attempt to defraud us, and not all are electronic (think, for example, about bogus callers at the front door claiming to be someone they are not, or about counterfeit goods).

We'll then move on to talk about information risk management – what it is and how it can be applied to mitigate the risk of fraud. Lastly, the paper will provide an overview of the products and services that RSA offers and how each of them helps to underpin an anti-fraud strategy.

The Fraud Landscape Today

Unfortunately the business of internet-based fraud has never been healthier.

When we think about the evolution of the internet and the new types of, and methodologies for, crime, that have developed, we can quickly come to one conclusion. The internet has not only enabled businesses to develop new routes to market and explore new business models, it has also done exactly the same for the fraudsters. In the case of the criminal underworld they have the added bonus of working in a completely unregulated global economy – a true free market! And let's be clear, we are not talking about so-called back-bedroom 'script kiddies' anymore, hacking for fun and kudos. These guys are full-time professionals, ably supported by an economy of goods and services that has evolved to support their needs.

It's this concept of criminals working in an economy, making their decisions based on return on investment (ROI) and ratios of risk vs. reward, that is the key to developing effective strategies to combating fraud. We need to affect the economics of the market, essentially seeking to make crimes unprofitable or too risky – too complex to execute, or giving too small a return, or having too much chance of being quickly detected.

The growing trend in the criminal world is to invest in and utilize 'crimeware', a class of malware specifically designed to commit financial crime, usually by stealing credentials or other personal information that ultimately enables money to be stolen. This class of malware is increasingly difficult to detect by those infected (either at or after the time of infection). It is often missed by anti-virus programs, and can execute increasingly sophisticated forms of attack, potentially in real time. It can bypass many security controls – in some cases it can even circumvent two-factor authentication.

As this criminal market continues to develop, and the efficiencies of a software-based approach are realized, we can expect to see these programs used against wider and wider varieties of organization, to perpetrate broader and more innovative forms of fraud.

We don't expect relatively unsophisticated attacks like phishing to go away, however. We expect to see them, and indeed already are seeing them, used against the perhaps less suspecting customers of smaller and more diverse organizations. Consider, for example, receiving an email request from your health club to update your billing records – would you think twice before clicking the link?

We need to affect the economics of the market, essentially seeking to make crimes unprofitable or too risky.

Against the more established, and therefore better-protected, targets for such crimes, the attacks will become increasingly sophisticated and will likely begin to employ multiple techniques simultaneously to maximize their effectiveness. We expect to see more ‘spear phishing’ – highly targeted attacks against specific individuals for key pieces of information. Consider what your response would be if you received a request, seemingly from your IT department, to reset your password to a specific database or system as part of a ‘security audit’. And I bet you’d respond if someone pretending to be from your human resources department urged you to update your bank details before the next payroll is run, to avoid the risk of not being paid that month!

Where RSA Can Help

There are lots of types of fraud, so it’s important that we agree some general (but by no means all-inclusive) taxonomy to explain where RSA can assist.

‘Internal’ Fraud

Organizations are at threat from two distinct sets of people. The first are those that we trust to be inside the perimeter of our firewall – generally an identifiable group, which uses the systems and equipment owned by the business. We’ll call these guys potential perpetrators of ‘internal’ fraud.

‘External’ Fraud

The second group comprises those on the outside trying to get in. As a society we are moving towards using online self-service channels to manage aspects of our daily lives. As a result, all sorts of organizations – originally banks, but now governments, tax and health authorities, utilities and more – are all exposing potentially sensitive and valuable information about us to the internet. The organizations providing such portals have a very specific problem in managing access to them, because by their nature they are internet-connected and it’s not often feasible to lock down the configurations and specifications of machines attempting to access them. We’ll call fraud that is attempted via such channels ‘external’ fraud.

RSA’s Role

RSA, and indeed EMC as a whole, is dedicated to the growth, leverage and protection of information infrastructure. At RSA we help manage the security of information, so it follows that we can help specifically where this information is crucial to the fraud being attempted. This information may be the target asset itself, as in the case of intellectual property theft; or it may be the key to unlock other assets, such as money from a bank account, insurance policy or credit card. Equally, it may be that manipulating information such as test results, or changing log files to cover the tracks of improper activity, are the root of a fraud’s success.

When we consider the threats which come from outside of the organization, it quickly becomes apparent that in many industries, what’s needed is expertise in protecting self-service portals. With the experience of protecting over 100 million online banking and brokerage accounts around the world, RSA is extremely well versed in understanding how such portals are attacked by fraudsters, and spotting potentially fraudulent behavior of seemingly authenticated individuals once they’re within the portal.

The Role of Risk in Mitigating Fraud

Fraud is essentially one class of risk to which business is exposed. So, where information is the asset we seek to appropriately protect from fraud, we can use a strategy based on information risk management to achieve the right outcome.

We have found that risk is the perfect basis for a conversation that clarifies and aligns business and IT security priorities. While risk management is, of course, not a new concept, RSA’s approach to managing information risk in an IT setting is distinguished by three key characteristics:

- Firstly, it’s information-centric. Information has become recognized as one of the most important assets in our economy and, as we’ve seen, it is increasingly key in

successfully perpetrating many types of fraud. Information has the potential to help you make money, save money, or get you in a whole lot of trouble. Focusing on information first and foremost clarifies business context, and following its path across the IT infrastructure reveals where it's potentially vulnerable.

- Secondly, it's risk-based. Using risk as a lens for security investment decisions ensures that the most significant challenges in mitigating fraud are addressed first.
- Thirdly (and perhaps most importantly, in that it differentiates RSA's approach from many others), it's repeatable. Our approach emphasizes the implementation of processes and solutions based on standards, frameworks and best practices that can be leveraged across multiple security and compliance initiatives – saving time, money, and effort.

The net result is that information risk management reveals where to invest, why to invest, and how security investments map to critical business objectives. Done right, this approach goes a long way to addressing the challenges we see information security functions facing.

I want to reinforce the point about being information-centric, because it is critical to why we think information risk management is such an effective strategy, not just for fraud prevention, but for providing a solid basis to tackle most, if not all, information-security challenges.

Every business or organization has some small number of critical business initiatives. It may be to drive new revenue growth, reduce costs, retain and improve customer relationships, keep the business running in the face of new adversities, or to stay compliant. Whatever the top initiatives are, there are IT projects associated with each of them.

For example, a partner-portal project supports a new channel to grow revenue. A process-outsourcing project seeks to reduce operating costs. An online community site seeks to build loyalty and retain customers. Information is generated, accessed, processed, stored and transformed as part of these projects.

That's the information you need to focus on –those most sensitive information assets that are critical to the business. Where and how do they travel across the IT infrastructure – across 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, in this case fraud, might take place? How likely are they to occur, and what's the downside, the consequence, if they do?

With this knowledge we can decide, based on the impact to the business, which risks we need to address and which we can ignore for the time being. And this will make security efforts much more effective and focused on what really matters.

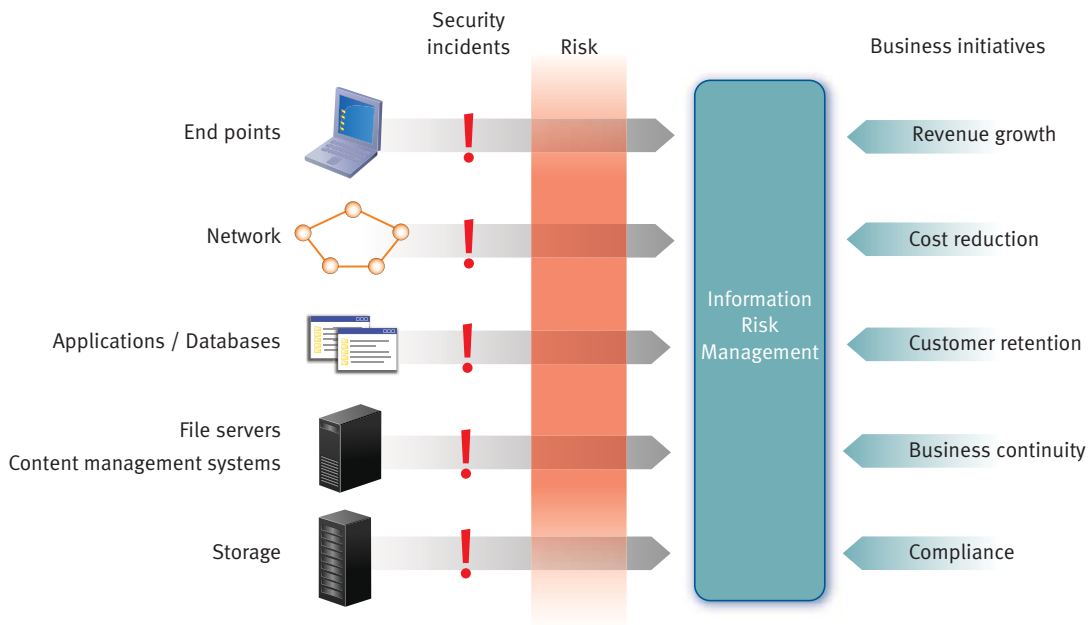
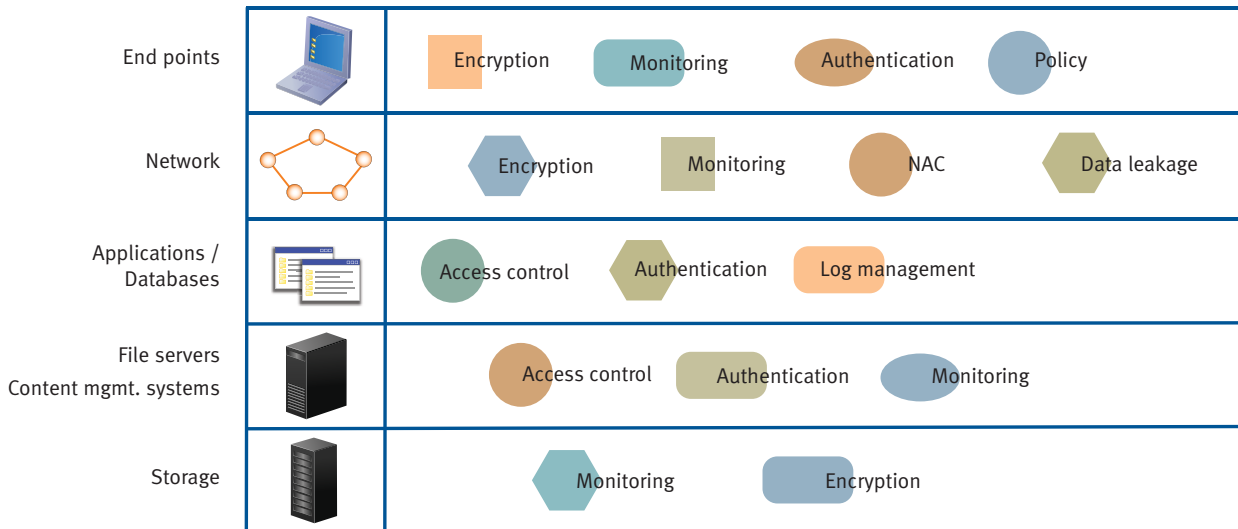


Figure 1. information risk management reveals where to invest, why to invest, and how security investments map to critical business objectives.

Figure 2. A typical siloed approach to security



So, to summarize, information risk management defines a strategy for:

- Tying IT security spending to business objectives
- Defining and identifying risk associated with sensitive information
- Determining what level of risk is acceptable to the organization
- Implementing a prioritized set of controls to reduce risk to acceptable levels

A Siloed Approach Creates Opportunity for Fraudsters

Organizations have traditionally implemented security controls reactively, in response to individual crises. So it is all too common to see businesses with silos of controls, often designed with similar objectives and technologies, but rarely effectively coordinated.

For example, one team may be chartered with ensuring that the company meets requirements associated with a particular government regulation, while another team is responsible for monitoring and enforcing internal policy compliance, while another is managing fraud. These teams probably won't be working together. In fact, they might not even be aware of each other's existence.

Because of these different security-focused silos, organizations also end up with redundant technology controls. For example, the PCI team may deploy a log-management solution to address its requirements, while another team deploys a similar solution in the context of Sarbanes-Oxley.

Implications of a Siloed Approach

When we think about the implications of such an approach, a financial impact quickly becomes apparent. According to Gartner, "allocating resources on a project-by-project basis means that enterprises spend an average of 150% more on compliance".¹

But beyond the purely financial impact associated with management in silos, there are numerous other implications:

- Redundant technologies: Firstly, there is the potential for redundant technologies to be deployed. In other words, organizations have several technologies – which essentially do the same thing – deployed in different use cases, increasing operational and management overheads and reducing business agility.

¹Gartner, "Gartner for IT Leaders Overview: The IT Compliance Professional." French Caldwell. October 22, 2007

- Inconsistent use of technology: Secondly, you end up with inconsistent use of technology controls, and inconsistent enforcement of policies and procedures. To follow our earlier example, the PCI team may be collecting certain types of log data, while the SOX team is managing logs more effectively.

When we think about fraud in this context, we find that wherever we have inconsistencies and silos, we introduce gaps, black holes and grey areas that fraudsters will quickly find and exploit. Indeed, our undercover fraud analysts often track conversations in underground chat forums between fraudsters who have found, and are exploiting, loopholes in a company's processes or technology.

When you adopt a framework approach, i.e. a holistic analysis, methodology and plan for dealing with security requirements, you are essentially putting a security program in place that enables your organization to solve these problems: you can take advantage of the commonalities between security and compliance programs, while at the same time reducing the opportunities for a fraudster.

According to a Forrester research project, which saw the organization interview ten chief information security officers


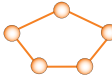



(CISOs), "regulatory compliance has resulted in considerable frustration for CISOs – they spend more time complying with individual regulations rather than taking a more strategic, framework-based approach. Most have realized that using a principles-based framework can help them not only address multiple regulations simultaneously, but also get a more comprehensive grasp on the security universe they are responsible for."²

A Framework-based Approach

There are many best-practice frameworks published in the information security industry today – each with its own pros and cons. At RSA, we tend to favor one – ISO 27002 – for its flexibility, comprehensiveness and the acceptance it has achieved worldwide.

Implementing an ISO 27002-based control framework is the optimal approach to controlling risk. Its comprehensiveness ensures that all aspects of risk are identified and addressed; it minimizes the costs associated with addressing risk by eliminating duplication; and it simplifies the process of responding to changing risk factors.

Figure 3. A framework-based approach to security

End points				Encryption		
Network				Encryption		
Applications / Databases		Monitoring Reporting Audit	Encryption Key Management	Encryption	Authen- tication	Data Loss Prevention
File servers Content mgmt. systems				Encryption		
Storage				Encryption		

²Forrester, "What's Top of Mind for CISOs in 2007." Khalid Kark. April 17, 2007

RSA's Solutions in Helping to Tackle Fraud

Having reviewed the theory, let us now look at the specifics of what RSA is able to offer in helping to tackle 'information-centric' fraud.

Key Tenets of an Anti-Fraud Strategy

If we think about security controls that help to combat fraud, we quickly come to realize that, in fact, these controls are much the same as those that are part of any effective risk management strategy.

We must:

- Know who is accessing our systems, and authenticate individuals, both by the credentials they are issued and when and how those credentials are used.
- Ensure that the integrity of data is protected, again authenticating access to it, but also encrypting it where appropriate. Log files need specific attention, because it is these that may provide the history that would uncover, and provide evidence to successfully prosecute, a fraudster. Ensuring that these have not been compromised is of paramount importance.
- Put in place systems that identify and mitigate accidental or deliberate data leakage or loss. Discovering unmanaged or unauthorized data residing in the network can in turn uncover potential fraudulent activity. Discovering unauthorized attempts to copy, distribute, print or otherwise remove data may do the same.
- Constantly monitor for alerts to security incidents generated by the various layers of infrastructure in the business.
- Provide auditable trails of activity to help provide the necessary evidence for use in any subsequent prosecution.

RSA can assist in all of these areas.

Identity Assurance

Our access controls support an essential process we call identity assurance.

Identity assurance enables organizations to create new business models that take full advantage of a worldwide community of empowered and protected people. With identity assurance, employees, partners and customers freely and securely interact with systems, identities, and

information, opening the door for new ways to generate revenue, satisfy customers, and control costs.

There are four major technologies required for identity assurance, and RSA provides products and solutions for each.

First is credentials management. It defines identity policy and manages the lifecycle of credentials used for authentication.

Second is authentication. We authenticate internal and external users of systems and resources using a broad choice of authenticators, via hosted, appliance, or on-premise applications.

Third is contextual authorization. We can manage access and federate identities (enable 'trust' around an authenticated identity to be shared electronically between multiple third-parties), enforcing policy across web resources, portals, and applications.

Fourth, we wrap these in a layer of anti-fraud intelligence, provided by analysts in our 24x365 Anti Fraud Command Center, to make the process more effective, mitigating identity misuse and abuse and gaining intelligence on emerging threats from the fraud underworld.

Data Security System

RSA has three product suites that implement controls for data.

RSA's Data Loss Prevention Suite prevents the unauthorized outflow of highly sensitive data from your network and endpoints. It addresses content in use (on end points), content in motion (carried over the network and created by applications such as email and web portals) and content at rest (in databases, file servers and storage).

RSA's Encryption Suite encrypts sensitive data at multiple points in the infrastructure and manages the lifecycle of encryption keys across the enterprise. We have developed encryption solutions for applications, file servers and storage, and offer partner solutions for end-user devices, databases, and network traffic.

RSA's Information Rights Management Suite enables secure document-sharing across an extended enterprise. It provides persistent protection, controlling rights on documents and emails through their entire lifecycle.

Security Information and Event Management

The key technology for reporting and auditing is security information and event management (SIEM). The RSA enVision® platform is our SIEM solution.

The RSA enVision platform captures all the event data and audit logs from the network, security, host, application and storage layers of the enterprise and transforms this information into valuable intelligence. From a security operations perspective, this information can be used in real time to alert security administrators to 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 such as GLBA, HIPAA, PCI and many others.

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

Summary

An effective and efficient fraud-prevention strategy is built on the same firm, framework-based footing as any information security strategy – at least in those instances where access to information is key to the success of the fraud.

The growth across many industries in opening up business processes to access by third parties, whether they be customers, suppliers or other third parties, inevitably expands the opportunity for fraudsters to exploit these channels of access.

Perimeter-based strategies, reliant on the principles of assuming that all inside the perimeter are ‘good’ and all outside are ‘bad’ fail totally when it comes to effectively fighting fraud. We need to protect sensitive information wherever it resides, by taking an information-centric approach.

Lastly, the implementation of a framework-based approach, such as that offered by ISO 27002, minimizes gaps and loopholes that fraudsters can otherwise seek to exploit.

RSA is able and willing to assist you in developing an effective strategy for mitigating such risks, and looks forward to working with you in the future to do so.

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.



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

The Security Division of EMC

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

IRMFF WP 0708