

# solutions RSA's strategy for information risk management

Taking a holistic, risk-based approach to IT security  
By Christine Kane

After years of viewing information security as a defensive strategy, designed to prevent bad things from happening, enterprises are starting to demand more from their security investments. They recognize that security can also contribute to an organization's success by helping drive key business initiatives, such as accelerating innovation and collaboration and reducing compliance costs. (See "From Brakes to Breakthroughs", page 8.)

But before this transformation can take hold, says RSA's Steve Preston, organizations must surmount the shortcomings of today's fragmented approaches to security. "Most organizations are in a reactive mode when it comes to security threats and industry regulations, and they struggle to manage security with point solutions," says Preston, senior director, Solutions Marketing, RSA. "The problem with this 'silo' approach is that good efforts in one area can be quickly nullified by failures in another."

Preston offers the example of a bank that has effectively deployed technology to protect its online banking portal from fraud only to have a privileged user copy confidential customer data to an unsecured laptop which is eventually stolen. The loss has to be disclosed, and the customer trust that has been gained with anti-fraud technology is completely undone by a lack of policy enforcement in the back office. Preston likens this situation to the carnival game Whac-a-Mole. "You hammer the problem down over here and it pops up

again over there. IT needs to engage the business in a way that not only puts security into relevant business context but also helps IT prioritize where to invest in security."

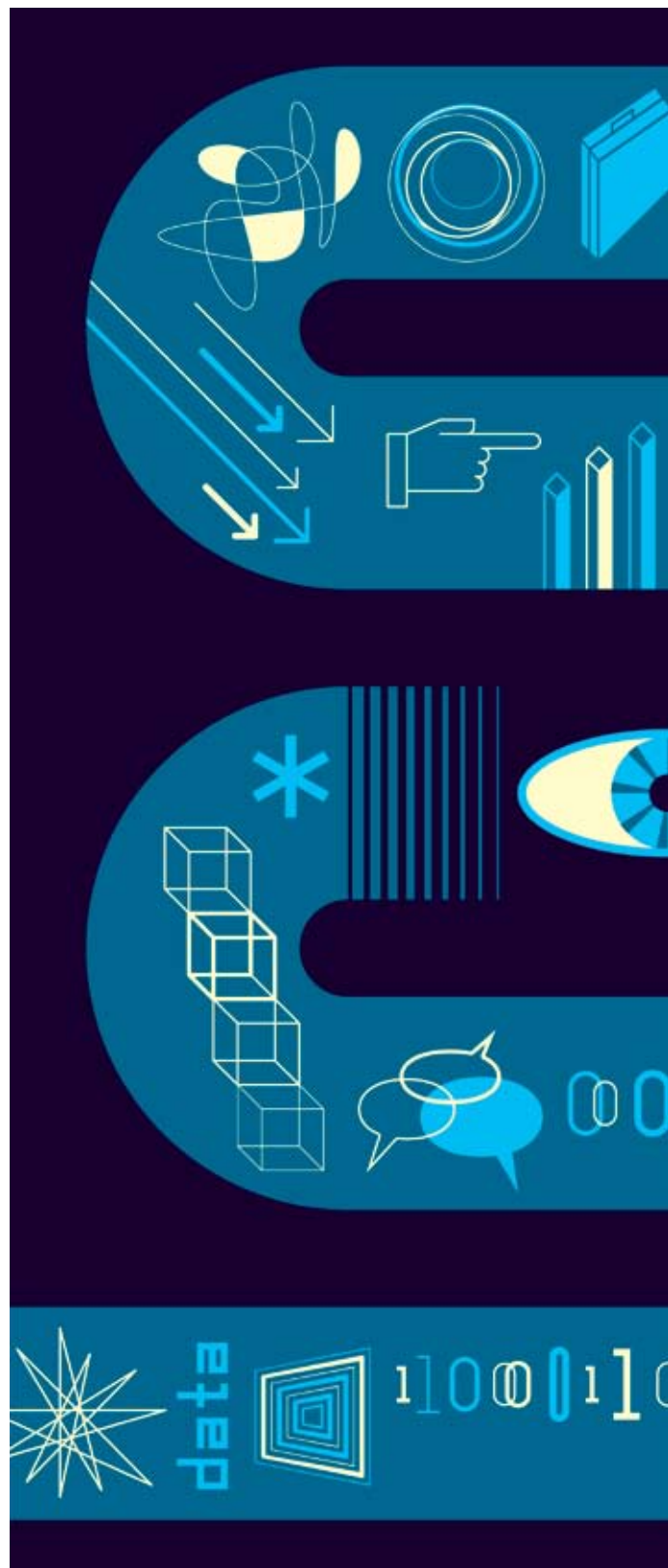
#### ADVOCATING A NEW APPROACH

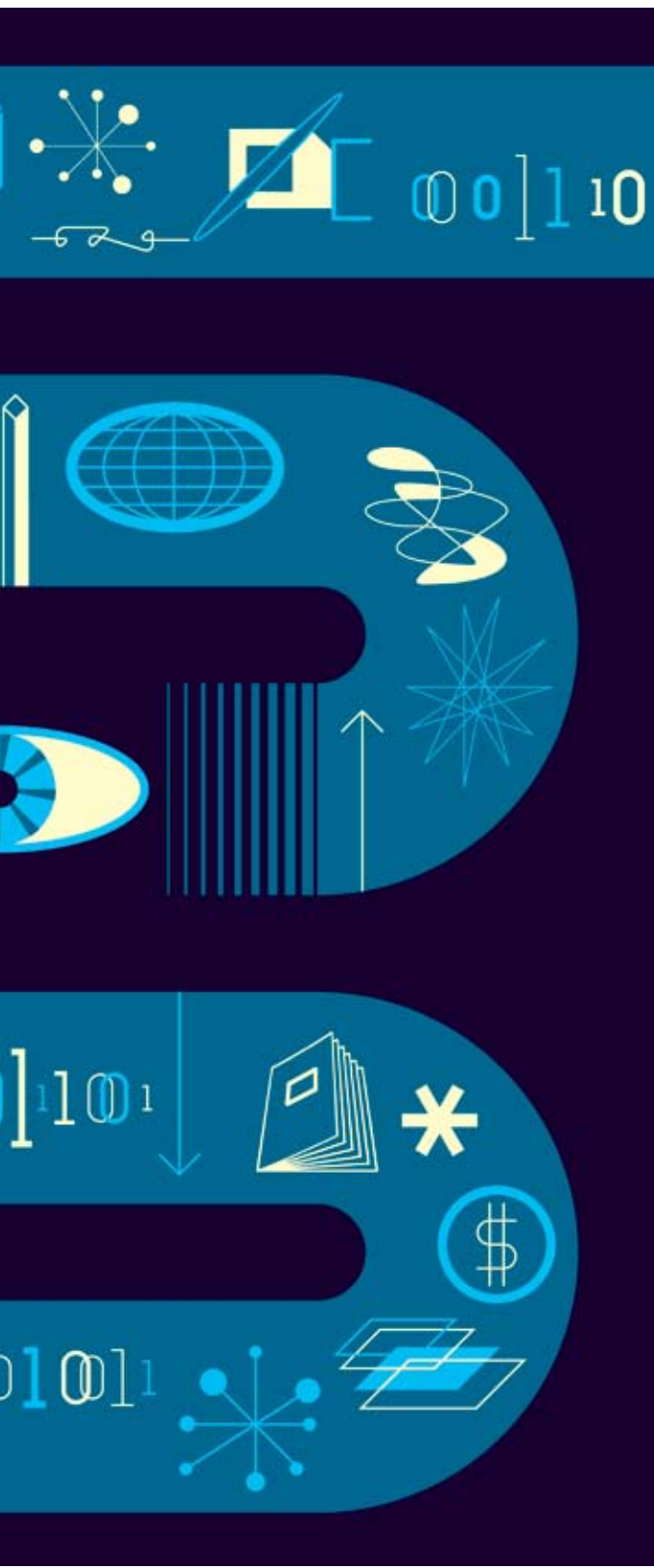
Faced with these realities, industry watchers and thinkers have called for a more holistic approach to information security and compliance, one that is based on the established discipline of risk management.

In the study "Information Risk Management in Financial Services," TowerGroup Senior Analyst Rodney Nelsestuen writes: "Practicing a holistic approach to security and information risk assures that business information contributes to achieving marketplace and business goals. ... Policy, practices, and technologies that provide a defense for information also can support the business's offensive strategy."

#### ENLIGHTENMENT STARTS HERE

Making the transition from today's "silo security" represents a significant shift for organizations, says Bob Blakely of the Burton Group.





“There is a process of enlightenment that organizations need to go through to effectively manage any kind of risk, including information risk,” says Blakely. “This process starts with understanding that risks have to be consciously managed and processes have to be put in place to assess an organization’s risk appetite, current risks and vulnerability. You then need to design controls that mitigate risk within one’s appetite. And you have to assess the effectiveness of those controls to be sure you’re operating within your tolerance while also achieving regulatory compliance.”

“The finance industry – and, to a lesser extent, the healthcare and energy industries – are the first industries to have reached this point of enlightenment,” he says. “With the rollout of its Information Risk Management strategy, RSA is helping organizations evolve to this stage of awareness and put in compensating controls using tools such as data loss prevention, encryption and authentication.”

### THREE CORE PRINCIPLES

Introduced last fall for the financial services industry and now being offered to other industries, RSA’s Information Risk Management strategy provides an end-to-end, holistic approach for protecting a business’s most critical information assets. (See sidebar, “RSA’s Comprehensive Approach.”)

“There are three pillars to our strategy,” says Preston. “The first is RSA’s information-centric approach to security, where you begin by understanding what information is critical to key business initiatives, such as growth through acquisitions or expanding partnerships. Then you diligently ‘follow the data’ to gain a more holistic view of all the places where it exists across the organization, where the points of vulnerability are, and what events

“Many people think risk management is about risk minimization, and it’s not. It’s about risk optimization. There are some risks you want to take because the payoff is so great; the challenge is to mitigate your risk to a tolerable level. A good risk management program allows you to take risks that your competitors can’t.”

BOB BLAKLEY  
ANALYST, BURTON GROUP

could put your business at risk.”

This is a very complex task. Data resides in many places, it’s mobile, it’s constantly being transformed, and it’s at the center of collaborative processes. “Tools for data discovery and classification are a critical part of our solution because they make our strategy actionable,” says Preston, explaining that the tools provide a basis for applying policy consistently across the universe of corporate information.

### PRIORITIZING INVESTMENTS

The second core concept behind RSA’s strategy is the idea that security investments should be prioritized, based on the amount of risk a given activity entails relative to the potential business reward, and in keeping with the organization’s appetite for risk. In this context, risk is defined as the likelihood an event will occur and the consequences if it does.

“The first thing a lot of people want to talk about is tape encryption,” says Preston. “In other words, many companies are putting locks

## solutions

on doors that almost no one is walking through. This results in over-scoping and misaligned investment in security. What organizations need to do is enable their highest priority business initiatives by protecting the information that is most valuable at the points where it is most vulnerable.”

Many analysts agree, including Blakley. “Many people think risk management is about risk minimization, and it isn’t,” he says. “It’s about risk optimization. There are some risks you want to take because the payoff is so great; the challenge is to mitigate your risk to a tolerable level. A good risk management program allows you to take risks that your competitors can’t.”

### ENSURING REPEATABILITY

Once enterprise information has been located and a risk assessment performed, the next step is to implement controls — including policies, technologies, and tools — to mitigate that risk. Here, repeatability and reuse of security controls is central to RSA’s strategy.

“You get repeatability from using



**BRYAN PALMA** of EDS says that many enterprises are ready to embrace information risk management.

common, standards-based frameworks and best practices,” says Preston. “Frameworks like ISO 27002 and the PCI Data Security Standard let you build to the gold standard, get you 80 to 95 percent of the way toward building your controls, and help eliminate unnecessary

or redundant controls.” Preston says his group has been systematically documenting how RSA and EMC products map to key frameworks so customers can be apprised of built-in controls that are already compliant.

Gartner Group has pointed out that the number of security controls an organization deploys is a good proxy for the complexity and cost of its compliance program. Some companies using a risk-oriented approach to compliance report that they have eliminated 30 to 70 percent of their controls, which

contributes to lower costs, reduced complexity and improved reliability.

### TAKING STOCK OF RSA’S STRATEGY

Are people ready to embrace security as a business accelerator? “I’d say roughly 20 percent of enterprises already ‘get it,’” says Bryan Palma, vice president, Global Information Security for EDS, which partners closely with EMC/RSA on many outsourcing and systems integration opportunities. “Another 60 percent are ready for that message but are not fully on board, and the remaining 20 percent are still back in the mindset that security is an inhibitor.”

Palma believes that RSA is well positioned to help companies move to the next stage of understanding and enablement. “On the tactical side, RSA has strengths that align with where the market is heading. These strengths include their expertise around data security, their focus on application security from an encryption standpoint, and their work in identity assurance and credentialing — both in consumer and enterprise markets. These are real differentiators.

“On the strategic side, RSA has benefited from being acquired by EMC, in terms of how well they work with enterprise customers, how they understand the business side of security, and their openness to partnering with integrators, service providers and technology vendors.” ■

## RSA’S COMPREHENSIVE APPROACH

*RSA brings together all the components an organization needs to plan and implement an Information Risk Management strategy. The five main aspects to RSA’s approach include:*

① **A GLOBAL RISK FRAMEWORK** Security is aligned with key business initiatives. For critical data, a risk assessment provides a holistic view of risk across lines of business and operations. Policy is developed based on best practices.

**OFFERINGS INCLUDE:** Risk Assessment Services, Policy Review and Development, Security Assessments.

② **INFORMATION CLASSIFICATION AND DISCOVERY** Information is classified so appropriate policies and protections can be systematically applied. Data and application discovery tools are used to locate all instances of sensitive information across the enterprise.

**OFFERINGS INCLUDE:** Information Classification, Information and Application Discovery.

③ **CONTROLS ON PEOPLE** Policy is automatically enforced by implementing controls such as authentication and access management that enable users to securely access enterprise resources and perform transactions while balancing risk, cost and convenience. Controls are based on standard frameworks, such as ISO 27002 and PCIDSS, enabling repeatability.

**OFFERINGS INCLUDE:** Credentials Management and Credentials, Authentication, Access Management, and Integrated Intelligence (transaction monitoring and adaptive authentication).

④ **CONTROLS ON DATA** Automated controls are implemented to protect structured and unstructured data, whether it is in use, in motion or at rest on endpoints, networks and servers.

**OFFERINGS INCLUDE:** Data Loss Prevention, Encryption and Key Management, Information Rights Management.

⑤ **REPORTING, AUDIT AND COMPLIANCE** Compliance with security regulations and policies is validated by auditing controls and documenting their effectiveness.

**OFFERINGS INCLUDE:** Event Management, Compliance Reporting.