

Financial Services

Risk-based information security: When “good enough” is good enough



Growing government regulation and increasingly lethal cyber crooks are forcing financial services organizations to redouble their data protection efforts. But amidst seas of data, how do you decide what to protect? BearingPoint explores a risk-based approach to data security that directs attention and resources to the most dire threats.

In this point of view

Introduction: What data should we protect?	2
Addressing a growing problem	2
Finding an alternative to “Rambo” security	3
Exploring the case for a risk-based security strategy	4
Focusing security efforts with a risk-based model	4
Understanding that you don’t have to do it all at once	6
Risk management drives improved business performance	7
About the authors	7

Introduction: What data should we protect?

Financial services firms hunger for customer information. The more they know about customers, the greater their ability to deliver the right products and services and build stronger customer relationships.

But woe to the institution that lets such information get into the wrong hands. Every corporate security breach that lets in cyber criminals, such as the recent high-profile theft of credit card information from customers of the TJX Companies' department stores, heightens regulatory scrutiny. And any company that is the unfortunate victim of such an attack faces untold reputation damage.

Financial institution executives recognize the need to protect customer and business information, in the most personal way. Regulatory sanctions and a media nightmare not only wreak havoc on the corporation, executives also can face personal liability, fines and even jail time.

But institutions simply can't protect all the data stored in disparate corporate systems. Often they don't even know what data exists and where it's stored. Even if they do, the cost and effort to secure all of it is prohibitive.

And, in fact, wasteful. Not every data item needs to be bulletproof. Not every regulation issued by numerous jurisdictions around the world demands immediate 100 percent compliance.

The question institutions face is deciding what information is most dear and demands extraordinary security and what can be less rigorously protected. BearingPoint believes a risk-based approach can help financial services organizations apply the appropriate levels of security to maintain regulatory compliance, secure vital data from attack and help protect corporate reputation.

BearingPoint believes a risk-based approach can help financial services organizations apply the appropriate levels of security to maintain regulatory compliance, secure vital data from attack and help protect corporate reputation.

Addressing a growing problem

Consumer identity theft is increasing at a disturbing rate. According to Gartner, unauthorized credit card charges rose nearly fourfold from 2005 to 2006 to an average of \$2,550. About 15 million Americans were victimized by some form of fraud related to identity theft in the 12 months ending August 2006. At least one-third of illegal bank account transfers, credit card and ATM/debit card withdrawals and purchases result from various kinds of electronic data theft.¹

Many jurisdictions are responding to this growing problem with legislation such as California's Database Breach Notification Act (Senate Bill 1386, codified at sections 1798.29 and 1798.82 of the California Civil Code). Senate Bill 1386 requires that any organization (agencies and businesses) that processes and stores personally identifiable information must publicly disclose security breaches involving unencrypted data in a timely fashion. Failure to disclose or untimely notification of a known breach can result in a civil lawsuit.

¹Avivah Litan, *The Truth Behind Identity Theft Numbers*, Gartner Research, February 2007.

Public disclosure of data-theft incidents can have significant and lasting impact on a company's reputation. This can erode competitive strength and market share. It becomes more difficult to retain existing customers, let alone attract new ones.

The TJX Companies breach is one in a string of incidents that have exposed sensitive customer information. Retail and financial services firms continue to be prime targets for those seeking to exploit the troves of personal consumer data. As a result, executives of firms that collect, store, process or transmit sensitive customer data find themselves at risk on two fronts:

- **Compliance risk**—the risk of organizational, and perhaps personal, prosecution for not complying with the data security and privacy aspects of applicable legislation.
- **Reputation risk**—the potential impact that public disclosure of a data breach can have on a company's reputation and brand image.

Finding an alternative to “Rambo” security

The demanding regulatory environment and growing information threats are forcing financial institutions to explore new data security strategies. However, the breadth and complexity of the problem and the staggering array of solutions available—to say nothing of the price tag—are daunting.

Part of the problem relates to the data itself. It's difficult to improve data security and privacy if you're not sure exactly what types of data are critical or where data is located. A large financial services organization could easily have hundreds of customer information databases, data marts and data warehouses spread throughout a worldwide enterprise.

For some institutions, the problem can be even more fundamental—not knowing what personally identifiable information actually is and, therefore, what needs to be protected. Many organizations have difficulty communicating data security policies and procedures—including defining personally identifiable information—to thousands of employees. Employees must read and understand the communications, and then actually follow the policies and procedures.

Organizations have frequently tried to address such challenges by throwing technology at the problem. A data security and privacy technology solution typically would involve policy management and enforcement tools, along with data encryption and user authentication technologies.

BearingPoint has found that many of these tools are designed to address mid-market requirements and don't scale well to meet the needs of large, global enterprises. In addition, many have been designed too narrowly, addressing only individual aspects of the enterprise data topology rather than an overall data security process.

To compensate for shortcomings in the tools, IT organizations often opt for a “Rambo” approach to data security: encrypt everything!

This approach presents its own problems. Even authorized users can have trouble seeing data. It can be difficult to determine what impact encryption has on other business processes and supporting systems. Encryption can slow application and system performance, potentially frustrating users. And, it's simply overkill. The institution finds itself paying far too much for way more than enough security.

BearingPoint has seen financial services institutions strike the right balance by taking a risk-based approach to data security. Since you can't do it all, you have to pick your battles or, in this case, pick your risks.

Exploring the case for a risk-based security strategy

With so much legislation globally—some overlapping, some contradictory, all complex and expensive to address—organizations are recognizing that it's virtually impossible to be 100 percent compliant. Further, the perfect technology solution for data protection simply doesn't exist.

But by and large, executives are not looking for the perfect security technology or the perfect governance model. They simply want to avoid running afoul of regulators or having a security breach turn into a devastating public black eye. They want to clear a minimum bar for information privacy, data integrity and business continuity. Good enough is good enough.

BearingPoint has seen financial services institutions strike the right balance by taking a risk-based approach to data security. Since you can't do it all, you have to pick your battles or, in this case, pick your risks. Determine what the biggest risks are, and focus your investments and effort there first.

Regulators support such a view. New guidance from the Public Company Accounting Oversight Board (PCAOB), the Securities and Exchange Commission (SEC) and the Federal Financial Institutions Examination Council (FFIEC), for example, calls for companies to take a risk-oriented approach to reduce the complexity and cost of compliance programs.

Protecting data to manage compliance and reputation risks requires a conscious business decision regarding three possible courses of action:

- **Avoid the risk**—find an alternative to the process that is exposing the data and creating the risk.
- **Mitigate the risk**—implement people, process and technology solutions that better protect the data, thereby reducing or eliminating the risk.
- **Accept the risk**—and face the potential consequences.

A risk-based approach to data security can help institutions choose among these options and decide where to invest their security dollars.

Focusing security efforts with a risk-based model

A risk-based security model allows an organization to create a strategic vision for data security and privacy, while providing a tactical framework for efficient, cost-effective implementation of data security solutions.

The premise underlying the model is that, for every business process, an organization should identify the minimum threshold of data security required to meet compliance requirements and protect the enterprise's reputation. An "acceptable risk bar" represents this threshold (Figure 1).

Activities, process changes and security solutions listed below the bar must be undertaken to achieve that minimum level of acceptable risk. Those above the bar would provide even greater security, but involve cost and effort beyond what's required to meet basic risk management goals.

From a funding perspective, anything below the bar would typically be a corporate level decision. Activities above the bar would represent discretionary spending, perhaps at the business unit level.

Figure 1 is an example of a hierarchical list of security actions, processes and technology solutions. Every organization sets its own acceptable risk bars at the corporate, business unit and process level based on its desired risk profile.

Setting the acceptable risk level involves understanding your risks, identifying the full range of possible steps to address risk and setting the bar for acceptable risk. Then you must implement the essential set of steps addressing the people, process and technology requirements to protect data at rest and in transit—where it’s originating, where it’s stored, where it’s going and how it’s getting there.

Figure 1. Risk-based data security

<p>We want to do. Brand protection, regulatory commitment, high potential to become regulatory commitment or support of longer-term plans for product differentiation.</p>	<p>Information privacy</p> <ul style="list-style-type: none"> Data protection Anti-money laundering (AML) Stronger authentication Encryption Offshore Entitlements Roles-based access control 	<p>Theft and fraud</p> <ul style="list-style-type: none"> Data protection AML Stronger authentication Encryption Offshore Entitlements Roles-based access control Developer access to production 	<p>Reputation</p> <ul style="list-style-type: none"> Data protection AML Stronger authentication Encryption Offshore Entitlements Roles-based access control Developer access to production
<p>We need to do. Regulatory commitment. Significant risk not to make planned progress; funding sources include corporate and business.</p>	<ul style="list-style-type: none"> Developer access to production 	<ul style="list-style-type: none"> Developer access to production 	<ul style="list-style-type: none"> Developer access to production
<p>Compliance/Regulatory/ Franchise Risk minimum “bar”</p>			

Project	Project scope
Developer access to production	Access control, authentication, provisioning/deprovisioning
Security event management	Reporting on security events and follow-up actions and processes to remediate
Data protection	Secure e-mail, data classification, secure file storage, secure file transfer, Internet Protocol security (IPSec)
Identity management and access controls	Roles-based access, authentication, provisioning and deprovisioning, multifactor authentication
Third-party information security	Securing how partners handle my data
Common risk assessments	Evaluate all projects from a consistent perspective
Data disposal	Establish and protect how we dispose of critical information
Enterprise access and authentication	Biometrics, physical security for grounds, buildings and rooms

Understanding that you don't have to do it all at once

Regulators do not expect financial institutions to be impenetrable to every attack tomorrow. Instead, they're looking for good-faith effort, a measurable plan for attaining compliance goals and continuous progress and reporting.

Because of this, an important tenet of the risk-based security model is a deliberate, measurable, stepwise approach to addressing risk. The entire transformation—implementing *all* possible steps—doesn't have to take place as one big bang. It's too expensive, complex and risky.

A risk-based information security model, to which BearingPoint refers as a "security infostructure," provides a platform for identifying the required components (Figure 2). Such an approach addresses key issues related to policy management and enforcement, data protection, identity and access control, and security transformation.

Developing a security infostructure involves:

- Understanding business requirements that drive creation of common components
- Developing the tactical road map to build those components as prioritized by business needs
- Creating a feedback loop to support future related projects

Figure 3 illuminates the benefits of using a security infostructure model to guide risk-related projects.

Figure 2. Security infostructure

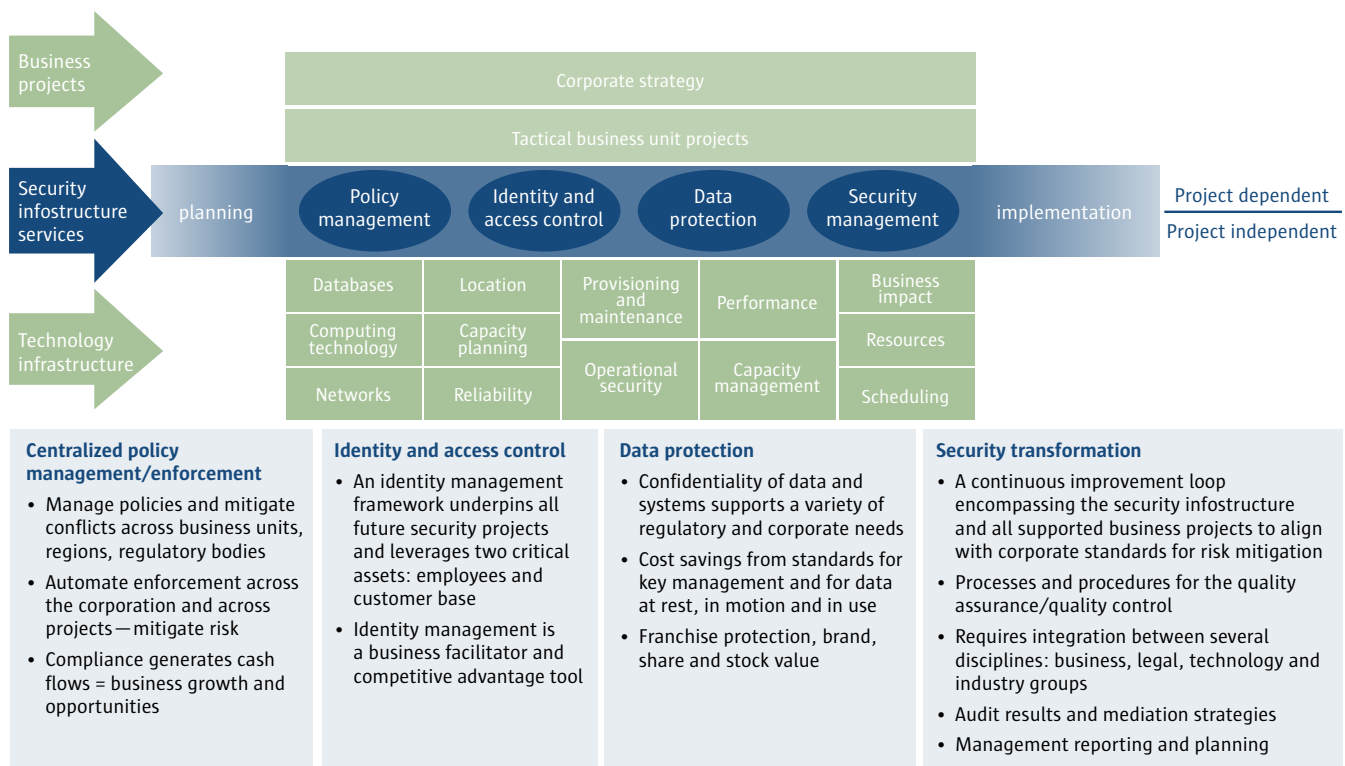
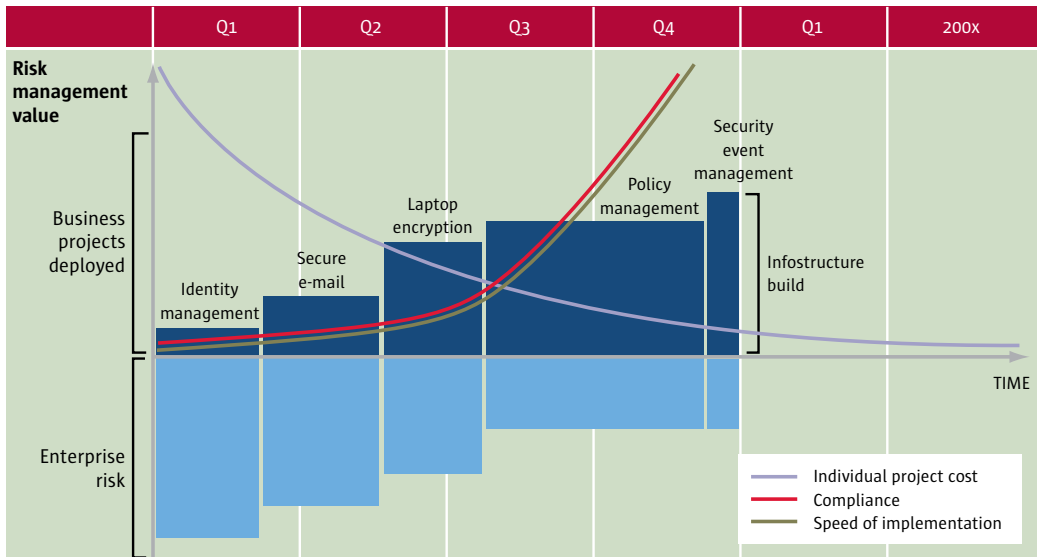


Figure 3. Controlling risk with a security infostructure



Implementing projects based on the security infostructure model can help lower the cost and time required to implement projects over time. The cumulative effect of successive implementations supports building a solid process and technology platform for data security. With lower per-project costs and faster implementation, business projects can be used to competitive advantage. The institution can generate new business opportunities ahead of competitors and open new markets for revenue growth.

Risk management drives improved business performance

Many organizations consider compliance activities to be essential, yet too expensive and time consuming. Taking a risk-based approach to data security and privacy — knowing when good enough is good enough — supports informed decisions about costs and benefits based on a clear understanding of risk priorities. The results? More reliable controls, lower audit costs, and fewer staff and resources required to maintain customer data privacy, meet compliance requirements and protect the corporate brand.

About the authors

Warren Zafrin leads the Information Security team within BearingPoint’s Financial Services practice. He has more than 18 years’ experience helping global banks and exchanges transform leading-edge technologies into products and services. He works with clients to help them protect their data, comply with federal and international laws and regulations, and reduce operational risk.

Peter Robinson is a senior manager in BearingPoint’s Financial Services practice. He has more than 10 years’ experience in data security and business analysis. His work in the data security field spans numerous technologies, including public key infrastructure and other encryption techniques, authentication, regulatory and policy enforcement, client-server solutions, and Web-based applications.



Management
& Technology
Consultants

Helping our clients get sustainable, measurable results

BearingPoint is a leading management and technology consulting company serving the *Forbes* Global 2000 and many of the world's largest public services organizations. Our more than 17,000 passionate, experienced consultants help organizations around the world solve their most pressing challenges, day in and day out. Through our collaborative and flexible approach, we help our clients get practical, sustainable, measurable results, make the right strategic decisions and implement the right solutions. We are BearingPoint, management and technology consultants.

To learn more, contact us at 1 866 BRNGPNT (+1 508 216 2523 from outside the United States and Canada), or visit our Web site at www.bearingpoint.com.

BearingPoint, Inc.
1676 International Drive
McLean, VA 22102

www.bearingpoint.com

© 2007 BearingPoint, Inc. All rights reserved. Printed in the United States. BearingPoint® is a registered trademark of BearingPoint, Inc. or its affiliates in the United States and other countries. Any other marks are the property of their respective owners. C3999-0507-01-USRD974