



WHITE PAPER

---

# VeriSign® Global Security Consulting

Security As a Competitive Differentiator





**CONTENTS**

+ Current Drivers of Security Spending: Compliance and Risk Management	3
Compliance	3
Risk Management	4
Where's the ROI?	4
+ The New Driver: Customer Trust and Differentiation	4
+ Building a Business Case for Differentiation	5
Business Strategy	5
Market Messaging	6
+ VeriSign® Security Services Overview	7
+ Conclusion	7
+ Learn More	8



# VeriSign® Global Security Consulting

## Security As a Competitive Differentiator

---

Until recently, investing in information security has been perceived as either a cost of doing business, or as a regulatory compliance issue. However, financial officers and chief executives are increasingly pressuring security professionals to justify IT security investments in terms of overall business goals and return on security investment (ROSI). Unfortunately, ROSI is difficult to calculate using classical return on investment (ROI) methodology, and budget justification has become difficult to demonstrate in many corporate environments.

An observable transition is underway. Current trends and empirical observations indicate that the use of security as a marketing differentiator may be a method of justifying and/or recouping investments in security. Consumers, business partners, corporate customers, and other organizations increasingly consider the protection of information assets—especially personally identifiable information (PII)—when evaluating companies with whom to do business. When a company markets its offerings as being more secure than that of its competitors, it differentiates itself, allowing security professionals to present a business case for security that addresses the traditional concerns and expectations of financial officers and other executives.

In this paper, VeriSign examines security in the context of the traditional goals and concerns of corporate decision makers: overall business strategy, ROSI, and market messaging.

### **+ Current Drivers of Security Spending: Compliance and Risk Management**

Compliance and risk management are the top drivers of information security spending today. With these drivers, justification for security spending is often based on scare tactics and anecdotal evidence rather than historical, hard metrics. As a result, information security can typically be viewed as a cost center rather than as a true value-add for business.

#### **Compliance**

Gartner's annual IT Security Spending Survey states that compliance remains the leading driver for increases in security spending.<sup>1</sup> Companies today must contend with not only internal, federal, and industry-specific regulations and policies, but also the varied security practices and requirements imposed by networked partners, suppliers, and customers. Meeting compliance requirements, servicing audits, and responding to unfavorable audit results significantly impacts most enterprises in terms of cost and effort. However, without the capability to effectively calculate a return on investment, budget justification is reduced to "we have no choice." The alternative—non-compliance—is not attractive either. Depending on the requirement, failure to comply or to provide auditable records can have serious financial and legal consequences. These consequences are in addition to the liabilities caused by compromised data, damaged branding, and loss of customer trust should a security breach occur.

### *Identifying Useful Metrics*

When considering the financial impact of security investments, it seems that security professionals have been better at predicting how a lack of security will affect the bottom line. Models exist for determining how much a security breach might cost in terms of fines, lawsuits, lost productivity, system downtime, compromised data, and so on. However, the industry does not have a reliable model for objectively quantifying how compliance and risk management positively contribute to a company's productivity, competitiveness, and the bottom line.

Granted, statistics and equations exist to help sell security to a company's financial decision makers, but they often have little or no statistical validity. In addition, many statistics are based on heterogeneous groups with too many variables in play to be truly scientific. For example, different companies use different methodologies to yield the figures they report for dollars lost to computer crime. One company may figure in system downtime, lawsuits, and lost sales, while another company may report only the actual dollar value of fraudulent transactions. Security research analyst Wes Sonnenreich argues for the creation of consistent standards for quantitatively measuring risk and risk mitigation; yet such standards are not on the horizon—nor will most companies ever collect sufficient historical security data to create statistically valid conclusions about potential future losses.<sup>2</sup>

### Risk Management

Risk management addresses security investment from the perspective that data, networks, and services must be protected in order to avoid costs associated with a security breach. Cost-justifying a risk management approach can be even more difficult than justifying compliance, as there is no external regulator or agency forcing the company to meet specific requirements. In establishing a security budget for risk management, companies often weigh the cost of security technology against the estimated losses they would sustain if they suffered a security breach. When estimating the cost of a potential security incident, security managers asking for funding often use best guesses rather than figures based on hard evidence. In addition, investing money in security to manage risk is like buying insurance—money is spent, without knowing whether the policy will ever be needed. The return on investment may never materialize and the security measures are viewed as simply a cost of doing business.

### Where's the ROSI?

Although reported costs of security incidents, fines for non-compliance with regulatory requirements, and other figures are valuable tools for justifying security investments in risk management and regulatory compliance, these metrics fail to address the traditional concerns and requirements of business managers, chief executives, and other officers. Increasingly, these decision-makers want to see value represented not only in terms of return on security investment (ROSI), but also in terms of how security relates to the company's overall business strategy and goals. CSOs, IT security managers, and other security professionals must improve how they articulate the value of security from a business perspective. Fittingly, the source of their solution may lie with the very people who consume or interact with their products, services, and networks: their customers, business partners, and suppliers.

### + The New Driver: Customer Trust and Differentiation

Reports of credit card fraud, identity theft, phishing, and other misuses of PII are on the rise, and consumers are increasingly wary of doing particular types of business online. In a survey of 6,000 U.S. consumers, Forrester Research determined that 20 percent of online consumers no longer open email that appears to be from their financial provider, and 26 percent did not apply for a financial product—because they were concerned about fraud.<sup>3</sup> In addition, a study by Princeton Survey Research Associates International found that 25 percent of Internet users no longer shop online, and 86 percent have made some sort of substantive change in their Internet usage due to risks of fraud and identity theft.<sup>4</sup>

As consumer awareness of data security and data confidentiality becomes more sophisticated, companies are beginning to view security from the perspective of their customers. As seen in recent advertising campaigns by Citigroup and others, technology and services providers are touting their investments in security and how their products and services are not just the better choice, but the safer choice. They are also promoting security to overcome reputation damage caused by security breaches and data losses. In doing so, these companies are discovering that information security can be a competitive differentiator. In fact, Forrester Research<sup>5</sup> reports that 74 percent of online consumers said that online security features will be an important consideration the next time they choose a financial provider.

**ROSI**

Historically, compliance and risk management have been difficult to justify in terms of ROSI. ROSI equations generally contain too many assumptions to generate accurate, objective figures, and many business managers have grown wary of ROSI algorithms. The good news is that many security officers do believe there is an ROI for security. In the 2005 Gartner IT Security Spending Survey, 25 percent stated that they used some sort of ROI model to justify security spending. As the survey author pointed out, these calculations often involve flawed logic<sup>7</sup>. Regardless, some of these concerns can be addressed by treating security as a competitive differentiator.

In spite of their drawbacks, ROSI equations—when used with well-defined metrics—can provide a useful starting point for creating positive arguments for security investments. What’s important is to identify and leverage what can be measured. Calculating ROSI for mitigating regulatory non-compliance risk, for example, may be quantitatively addressed rather easily as regulators have clearly delineated the financial penalties for non-compliance. To do so, one can use as a starting point the ROSI algorithm presented in Sonnenreich (2005):<sup>8</sup>

$$ROSI = [(E_R * \%M_R) - C_s] / C_s$$

where  $E_R$  = Risk Exposure,  $M_R$  = Risk Mitigated, and  $C_s$  = Solution Cost.

This algorithm may then be modified to reflect compliance investment and differentiation by 1) including the fiscal impact of regulatory non-compliance (fines, removal from preferred status list, etc.), and 2) adding any economic upside that results from releasing positive indicators of security controls and posture, so that

In business-to-consumer environments, using security to increase trust and differentiate products can help drive sales, build brand equity, improve online-shopping conversion rates, and increase the number of credit card transactions. In business-to-business environments, especially where regulatory compliance is an issue, this approach can encourage preferred-partner relationships, which often include financial benefits such as price discounts and favorable payment terms. In both the B2C and B2B environment, this approach may also elevate security from being a cost center to being a profit center, with demonstrable return on security investment (ROSI).

**+ Building a Business Case for Differentiation**

By focusing on differentiation and customer trust—and the positive returns these approaches yield—security managers can frame security in the context of business strategy and market messaging, and thereby present a stronger business case for security expenditures. The following sections focus on these components.

**Business Strategy**

When developing an information security program, security managers must strive to minimize risk and cost, as well as add value by allowing the company to differentiate its product or service and charge a premium price. How the company uses security competitively should map to how the company defines its business strategy. In the classic business text, *Competitive Strategy: Techniques for Analyzing Industries and Competitors*, Michael Porter identifies three generic business strategies: overall cost leadership, differentiation, and focus.<sup>6</sup>

**Overall Cost Leadership**

The overall cost leadership strategy revolves around effective cost control, and marketing products and services based on price. Southwest Airlines, Wal-Mart, and most other large-scale retail companies market themselves as low-cost and are extremely aggressive about controlling costs. Companies that use this strategy usually focus on maintaining adequate security at the most reasonable cost. However, they must also manage risks appropriately. For instance, a large retailer that processes millions of credit card transactions a month may have a limited security budget but also recognizes that a compromise to credit card data would cost the company a significant amount of business.

**Differentiation**

The differentiation strategy capitalizes on superiority and uniqueness. Companies like Mercedes-Benz and Rolex, which sell a higher-end product at a higher price, exemplify this strategy. Companies using security as part of their differentiation strategy advertise their capability to protect data and other assets, and they proclaim that they do it better than their competitors. For example, a financial services provider might give very little media attention to the banking features of an online application that it hosts—especially if its competitors offer a similar product. Instead it may focus on the application’s security features, which help differentiate the company and the application, and appeal to the customer’s need for trust. Advertising for the application might tout the following features and capabilities:

- Network security controls to prevent hackers, thieves, and disgruntled employees from accessing, stealing, or altering the company’s confidential data
- Superior data protection, including state-of-the-art encryption
- The capability to grant access to specific information only to those who need it
- A certification of trust that is issued by a third-party security firm

$$ROSI = \frac{[(E_R * \%M_R) + R - C_S - C_M]}{(C_S + C_M)}$$

where  $R$  = Revenue Effect and  $C_M$  = Marketing Cost.

Because the penalties for regulatory non-compliance are well known, we can remove the uncertainty from the Risk Exposure term. As for Revenue Effect, we can estimate the effectiveness of market messaging in terms of increased revenue, using a variety of empirical features identified in econometric time series models (e.g., Horvath and Franses 2003).<sup>9</sup> If security compliance status is used to differentiate a company's offering and thereby influence a market, the impact on revenue may be measured and used to augment the calculation of return on security investment. It is highly unlikely that the result of this calculation would be anything but non-zero and positive. Empirical data are not readily available; such information is generally classified as a competitive secret.

The following example is instructive: To completely mitigate the risk of being fined \$500,000 for Payment Card Industry (PCI) non-compliance, a financial institution spends \$250,000 to add security controls and contract a managed security monitoring service. The company then spends \$50,000 to make 1,000 targeted marketing impressions that advertise regulatory compliance as a competitive differentiator. At a five percent rate of return, the processor gains 50 new customers averaging \$10,000 each in revenue recognition over the lifetime of the controls.

Recent advertisements that promote security as a differentiator include Citigroup's identity theft ad and the various America Online commercials. These companies recognize that people are concerned about security and that customers will go to the company that claims to be the most secure.

### Focus

Companies use a focus strategy when they sell solely to one particular market segment or consumer base. A focus strategy can take a cost leadership approach or a differentiation approach. In the latter case, which occurs more often, the company can provide a better, more customized product to the consumer. An example of this strategy is an accounting software package (such as Sage Software's Timberline or Intuit® Master Builder™ software) that differentiates itself by addressing the specific needs of users in the construction industry. Similarly, a technology firm that does business with hospitals or a service provider that works with government intelligence agencies would be an example of a focus strategy that could then be differentiated by addressing the specific security and privacy needs of these organizations.

### Market Messaging

Effective messaging about security can help differentiate a company's offerings, strengthen product branding, and influence customer behavior. For this reason, it may be beneficial for product differentiation strategies to be closely linked to market messaging. When security is publicly articulated as a competitive differentiator, the following effects are possible:

- An increase in customer loyalty
- Stronger branding
- The addition of a positive differentiator to the competitive analysis process used by potential customers

Indeed, an April 2005 JupiterResearch report finds "strong evidence that banks can promote the security of their online offerings as a means of differentiating themselves from competitors and winning customers. The analysts found that in a climate of heightened consumer awareness and concern about online security and fraud, 37 percent of online banking consumers believe some banks are more secure than others, while 43 percent place online banking security among the top three factors in selecting where to bank."<sup>10</sup>

To help drive ROSI, security professionals must work closely with marketing departments to develop campaigns that highlight and differentiate the company's ability to protect information and other assets. In addition, they must track and analyze messaging, marketing budgets for security-focused ad campaigns, sales increases, boosts in public perception, and other marketing data to document the correlation between market messaging and increases in revenue or boosts in consumer perception. In doing so, they gain valuable data for justifying security expenditures.

The modified ROSI algorithm becomes

$$\text{ROSI} = [(\$500,000 * 1) + \$500,000 - \$250,000 - \$50,000] / (\$250,000 + \$50,000) \text{ or}$$
$$\text{ROSI} = 700,000/300,000 = 2.3$$

Therefore, using the preceding assumptions, the institution would recoup more than double the cost of the controls in new revenue, and that increase would be directly attributed to the imposition of the controls. The time scale relevant to the expenditure/marketing/recovery cycle may be defined based on whether the implemented controls actually do provide a competitive differentiator, and the magnitude of the effort needed to achieve the desired control condition (based on the starting point). A compelling differentiation would likely be achieved through the deployment of significant controls, combined with an attestation by an objective third party as to their efficacy; this effort would span at least one year.

As demonstrated here, when used creatively and in context, sales upticks, market perceptions, and other related metrics can help security professionals develop convincing arguments for using security to differentiate offerings, strengthen branding, and increase ROSI.

## + VeriSign® Security Services Overview

A security-as-differentiation strategy is successful only when customers trust the security that is being offered. Although many vendors offer security products and services, few providers match VeriSign's expertise, global intelligence-gathering capabilities, or status as trusted advisor. Indeed, the VeriSign brand has always been predicated on trust. As a leading provider of intelligent infrastructure services for the Internet and telecommunications, VeriSign has a proven record—backed by comprehensive service level agreements—of security, availability, and reliability. Its managed services allow enterprises to help mitigate the risks, complexity, and costs of building and maintaining in-house solutions, while retaining full control of user, network, and data security policies. By leveraging the trust associated with the VeriSign brand, companies may gain a unique differentiator when they promote their products and services to business partners and customers.

- **VeriSign® Global Security Consulting** – VeriSign Global Security Consulting combines seasoned practitioners, state-of-the-art tools, and world-class program management to deliver optimal security and compliance solutions. Our flagship offering, the VeriSign® Security Certification Program, provides a mechanism for organizations to communicate a superior commitment to security to their customer base. The VeriSign consulting team includes one of the highest concentrations of credentialed experts in the industry, and VeriSign security professionals are trained, certified, and experienced in the design, acquisition, and deployment of all major security solutions.
- **VeriSign® Managed Security Services** – The VeriSign suite of managed security services is a complete network security program that includes around-the-clock management and monitoring, real-time security intelligence, a global infrastructure, and a staff of 24/7 security experts to address today's increasingly complex network security threats.
- **VeriSign® Unified Authentication** – This VeriSign service provides a single, integrated platform for provisioning and managing all types of two-factor (strong) authentication credentials. Strong authentication can be a key differentiator for customers conducting high-value transactions online.
- **VeriSign® SSL Certificates** – VeriSign Secure Sockets Layer (SSL) certificates use the strongest possible encryption to protect Web sites, intranets, and extranets for online business, e-commerce transactions, and confidential communications.
- **VeriSign® Managed PKI Services** – VeriSign digital certificate-based services enable companies to secure intranets, extranets, virtual private networks (VPNs), email, and e-commerce applications while retaining full control of information access.

## + Conclusion

Security professionals can no longer justify IT security expenditures on the basis of risk management and regulatory/standards compliance alone. Financial decision-makers increasingly want to see how security fits into the company's overall goals for business strategy, return on investment, and marketing. As consumers become increasingly concerned about data security and the protection of their private information, IT managers are recognizing that security—when publicly promoted to build customer trust and differentiate products and services—can be used to build a strong business case for security investments. When implemented with industry-leading products and services from VeriSign, security solutions gain the additional value and differentiation of a brand that is strongly associated with security, reliability, and availability.



### *Market Messaging That Focuses on Differentiation and Security*

eFunds Corporation, one of the largest third-party payment processors and direct-debit database providers, promotes the message that the customer who “feels safe will spend more.” In addition, security is showcased throughout the eFunds Web site. This messaging, especially in light of recent high-profile compromises at payment processors, publicly articulates eFunds’ commitment to protecting consumer information.

America Online (AOL) airs a commercial in which a customer is navigated through a building while being protected from falling paint cans and construction debris. The cans and debris are referred to as spam, phishing, and viruses and represent the hazards of being on the Internet. The message is that AOL provides better protection from these hazards than its competitors.

Visa has an ad in which the offensive line of the New England Patriots represents the different measures of security and fraud protection offered by Visa. Quarterback Tom Brady represents the ordinary consumer being protected by these measures.

VeriSign is positioned in the Leaders Quadrant of the August 2007 “Magic Quadrant for MSSPs, North America, 1H07” Gartner report.

### **+ Learn More**

For more information about VeriSign® Security Services, please call 650-426-5310, email [enterprise\\_security@verisign.com](mailto:enterprise_security@verisign.com), or visit us at [www.Verisign.com](http://www.Verisign.com).

**Visit us at [www.Verisign.com](http://www.Verisign.com) for more information.**

- 1 Wheatman, Vic. User Survey: Security Summit Reveals Spending Patterns, Worldwide, 2005 Gartner, August 2005
- 2 Sonnenreich, Wes, Return on Security Investment (ROSI): A Practical Quantitative Model, March 2005
- 3 Forrester Research, Inc., E\*TRADE Battles Online Fraud with Strong Authentication, March 15, 2005
- 4 Consumer Web Watch, Leap of Faith: Using the Internet Despite the Dangers - Results of a National Survey of Internet Users for Consumer Reports WebWatch <http://www.consumerwebwatch.org/pdfs/princeton.pdf>
- 5 Forrester Research, Inc., op. cit.
- 6 Porter, Michael E., Competitive Strategy: Techniques for Analyzing Industries and Competitors. New York: Simon & Schuster Inc., 1998
- 7 Wheatman, Vic. User Survey: Security Summit Reveals Spending Patterns, Worldwide, 2005 Gartner, August 2005
- 8 Sonnenreich, Wes, Return on Security Investment (ROSI): A Practical Quantitative Model, March 2005
- 9 Horvath, C. and Franses, P., Deriving Dynamic Marketing Effectiveness from Econometric Time Series Models, 2003
- 10 JupiterResearch, Online Banking: Employing Security as a Differentiator, April 2005 11 eFunds Marketing Brochure, 2005

©2007 VeriSign, the VeriSign logo, the checkmark circle, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. The Magic Quadrant is copyrighted August 2007 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner’s analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the “Leaders” quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

00021326 05-30-06