



Dan Scheuble
President, Mortgage Division
Fidelity National Information Services

Security as a Core Business Strategy

In any industry where sensitive information is a critical part of day-to-day operations, most companies understand that security must be one of their core business strategies. Visionary companies dedicate a significant part of their IT budget and recruit talented professionals and business partners to help them protect customer information, secure operational data and defend their hard-earned brand equity against security breaches.

Yet, competing internal priorities and pressing market demands make it difficult for companies to determine how much to spend, how much protection is enough and where to draw the line between prudence and overkill.

Everyone is working with limited budgets and resources, and while IT executives know there is much more they could do, business executives may want them to do the job with less.

When approaching the issue of security, the executive team has three basic choices. They can choose to do nothing, hoping that the problem is overblown and the company will not be targeted by cyber-criminals. They can invest in a set of basic security solutions and expect them to provide sufficient protection. Or they can deploy highly sophisticated strategies designed to protect their corporate data from even the most aggressive attempts to steal it.

Cyber-criminals have a voracious appetite for confidential customer data. There are millions of well-documented cases of perpetrators using information to steal money from bank accounts,

open credit cards, apply for and get mortgages, and sell names and social security numbers across the globe. Other criminals (like terrorists) are primarily interested in disrupting or shutting down business operations, hoping to create as much chaos as they can.

Institutions that do nothing believe their standard security measures are adequate to protect their customer and business data and that the probability of it being compromised is low. In most cases, this means that "data-in-flight" (data being moved around) remains at risk, whether it is being transmitted electronically, or on media that is being transported by carriers. This is a dangerous position to assume, but not all companies believe a catastrophic loss of data will be the result.

The second choice is to implement another layer of defense that can provide a significant improvement in the security of an environment. Many companies deploy a secure network infrastructure armed with intrusion detection, strong authentication and at least some data encryption. These basic precautions are an excellent foundation for a secure enterprise and will substantially reduce the probability of compromised data.

The third choice is to implement an industry-leading, sophisticated data security program that invests in and deploys all possible precautions. These are expensive programs, but the companies that use them believe they are essential. They are very successful at protecting corporate data from theft, and can dramatically reduce the reputa-

tional and hard-cost risks associated with a security breach.

A thorough analysis of the processes and technologies companies use to collect, transmit, manipulate and store data allow them to understand their risks and develop defense strategies that can better protect both them and their customers. However, to effectively protect critical data across the enterprise, a layered security plan must be formulated, funded and implemented company-wide. The plan should identify the required IT infrastructure, standardize data-related processes and provide a method for auditing performance.

Encryption, though expensive, is also critical to thwarting criminal misuse should sensitive information fall into the wrong hands. It is being deployed by a growing number of financial institutions, especially for highly targeted customer information. Since our industry still relies heavily on transport carriers to move large volumes of data on tape, the risk factors are obvious (and thefts are highly publicized).

Companies that treat security as a core business strategy will win the trust and loyalty of their customers, and protect their valuable data assets and brand equity. The investments can be steep and the target is always moving. Still, securing corporate data is not an option. In fact, it is one of our most important responsibilities. ★



**FIDELITY NATIONAL
INFORMATION SERVICES**