

[Print This Article](#)[<< Return to It's time to think differently about protecting data](#)

It's time to think differently about protecting data

Bill Ledingham, CTO, Verdasys
September 10 2008

The recent rash of high profile security breaches, data loss incidents and associated fraud highlights the fact that the security industry is failing to meet the threats organizations face when it comes to protecting the lifeblood of their business – their data and their customer's data. As the threats of data loss continue to increase, it's time for IT, CIOs, CEOs, boards and security practitioners around the world to fundamentally reexamine their approach to security; and, instead make security a strategic, enterprisewide initiative.

Protecting data within corporations

The value, quantity and mobility of data has increased to a level where any lost or stolen laptop or mobile device can lead to a significant loss of highly sensitive information. The recent examples of data loss are numerous and well-publicized. An analysis of these breaches points to a combination of vulnerabilities and threats. Networks are porous – given the mobility of data there is no effective “network perimeter” to protect. Computers are porous – given the size and complexity of the Windows environment and applications, it's impossible to protect against all system vulnerabilities. Despite of a myriad and, some would say, confusing array of security products – anti-virus, firewalls, host intrusion protection, network monitoring, etc. – corporate systems are becoming compromised at an alarming rate, due in no small part to the growing sophistication and syndication of hackers and cybercriminals.

In addition to the external criminal threat, threats arise from insiders having access to increasing amounts of sensitive information. The risk of employees stealing information is real. Certainly, very little insider behavior is purposely malicious. However, through a lack of knowledge of information policies, improper training, perceived expediency or simple negligence, insiders can put sensitive data at risk. In addition, new information security demands arise as business models evolve. Ever-expanding supply chains, the growth in off-shoring and outsourcing, and the move to put more services and data online bring new potential for exposure.

The security industry is focused on the wrong problem. Data loss is not an infrastructure or network problem; it's about protecting a company's information where it's at the greatest risk – whenever and wherever it is in use. It is only at the point of use where data can be effectively controlled. The challenge – and where the focus should be – is on expanding the coverage of effective information controls that can be applied where data is used. These controls need to be extended beyond the corporate network; beyond the VPN; beyond assets that are under control of the corporation to areas where the corporation is not currently in control – suppliers, trusted third parties, consumers and public or shared resources such as cloud computing. Taking a comprehensive, holistic view is the only meaningful approach to reducing data loss incidents. Indeed, it goes far beyond the simple notion of data loss prevention, but fits within a broader framework of information control and risk management.

Extending data protection

Clearly, the problem is not limited to protecting data within the boundaries of the corporation – it extends from the corporation to the consumer. A major source of online fraud occurs via identity theft from stolen credentials obtained via phishing schemes or malware (viruses, trojans, botnets, etc.) resident on consumer machines. Through keyloggers, rootkits and other malicious software, criminals are able to steal user names, passwords, credit cards and other personal information from compromised PCs as consumers interact with online commerce sites and execute transactions.

The increasing sophistication of malware (e.g., the ability to mutate, hide from anti-virus software, etc.) has led to a marked drop in the efficacy of traditional prevention techniques. Leading anti-virus products, for example, have been shown to be less than 50 percent effective at discovering and eliminating the current malware in existence. The trends have led some analysts to suggest that anti-virus products will be obsolete within a few years. Analysts estimate that two-thirds of consumer machines are currently infected with some type of malware.

Companies must take ownership of the problem of how to protect data and transactions in compromised environments (e.g., consumer machines ridden with malware). Consumers have minimal exposure – \$50 maximum or no liability. Corporations are saddled with the problem of escalating fraud losses and the threat to online business models. Therefore, they must take a greater role in tackling the problem. The starting assumption in today's environment must be that a consumer machine is already compromised or soon will be. Given that, the challenge is how to protect data and transactions within this environment. A notion of “fingertip to server” is called for.

Securing the cloud

The challenges do not stop there. As companies begin to leverage cloud computing resources, especially social networking sites such as FaceBook or Twitter, the need for new ways to safeguard corporate data grows dramatically. The risks are two-fold:

1. A company is at increased risk of inadvertent or purposeful disclosure of sensitive data via posting to public sites; and,
2. There's increased exposure to malware as many of these sites are known distribution points.

The challenge is how to leverage the benefits of collaboration and lower costs while at the same time protecting data.

Analysts have proposed a trust model and policies that dictate fair use of social networking sites. In addition to usage policies for employee interaction on public sites, companies must look for new ways to protect data on resources that are not under their direct control. This includes securing data as it is transmitted to and stored in the cloud as well as granting the appropriate access rights to who can view the data.

Conclusions

Security vendors are not responding to these fundamental shifts. They have failed to recognize that almost everything in the business world has changed, much of it due to technology.

Given the range of requirements, a holistic, adaptable approach to data security is needed. The focus must be on the data – while network and application security will continue to have a role, the emphasis needs to change. Security policies need to follow the data and act where the data is used. As always, the challenge is how to secure the data without impacting productivity. If done correctly, data security can

actually be an enabler – allowing data to be used more freely across corporate supply chains and customer interactions while ensuring that the necessary safeguards are in place. Until the security industry embraces this data-centric approach, data losses will continue to surge.