

## **Developing a Data Leakage Strategy**

**By Andrew Plato, CISSP, CISM, QSA  
President / Principal Consultant  
Anitian Enterprise Security**

There is a lot of talk right now about data leakage protection (sometimes called extrusion prevention). Data leakage is an important information security issue facing organizations of all types. However, data leakage is particularly important for financial services, health care and any organization with PCI compliance issues. Unfortunately, like many hot topics, there is a lot of misinformation.

### **Understanding Data Leakage**

In simple terms, data leakage is when confidential or sensitive information is transmitted to an insecure or unauthorized source. The most common example of data leakage is when a user emails confidential company information (like an account number, health records, or other such data) to an untrusted third party.

There are many ways that data can leak from your environment. Web-based email, peer to peer networking, USB disks and botnets are all possible vectors for leakage. Data leakage is a complex challenge that affects your business at many levels. It is vital to develop an organizational strategy to handle data leakage.

### **Beyond Technology**

Data leakage is ultimately a business problem. While there are many important technologies involved in data leakage, before charging ahead and purchasing products, it is vital that you define a comprehensive data leakage strategy for your business.

Your strategy should address the following issues:

- Executive buy-in
- Security policies, procedures, guidelines & standards
- Acceptable use policies
- Email security & encryption
- Web access & filtering
- Perimeter security
- Network and host-based intrusion prevention & detection
- Endpoint protection (anti-virus, intrusion prevention, USB disk controls, etc.)
- Data identification, classification & integrity monitoring
- Log aggregation & event monitoring

Of course, the list above is a generic set of common issues. Your organization must customize a data leakage strategy to the specific needs of your industry.

However, before you charge ahead and purchase new technologies, its best to step back and take a look at what you already have. Anitian recommends conducting an informal survey of what products, policies and practices you currently have and how they can be optimized for data leakage issues. Many common security technologies, like web filters or IPS can provide many of



the same features as dedicated data leakage products. If you do decide to implement a dedicated data leakage solution, make sure you have addressed all of the issues on the aforementioned list.

### **The Human Factor**

Lastly, data leakage has one fundamental component that is not silicon-based – humans. A good data leakage strategy must begin with clear policies and guidelines for employees on what is acceptable use and proper methods for identifying and handling sensitive or confidential data. Those policies need to be effectively communicated to all affected employees, contractors and any third party involved in your business.

Naturally, Anitian Enterprise Security can help. Whether you are considering new technologies or need professional services to help develop your data leakage strategy, Anitian has the expertise you need.