



Feature

Data Protection and Security

Advice from CIO Laurie Pemrick

Laurie Pemrick CIO, McCrory & McDowell LLC

Highlights

- Internal control is one of the most overlooked areas of data protection
- Classifying information is one of the first steps in securing data
- Employees should have paranoia training to understand responsibilities



Data protection is often viewed externally. Firewalls, strong passwords, secure tunnels are all part of the picture. It is becoming more and more evident as time progresses that data protection has to start from the inside and work its way out. One of the most overlooked areas of data protection within firms of all shapes and sizes is internal control.

Most breaches occur internally and are largely overlooked. The breaches can be as simple as employees having access to more information than they need and run the gamut all the way to fraud and corporate espionage. While there are many ways to form internal control policies for an organization, consider the following information along the way.

One of the first steps in securing internal data is classifying information. Classification sounds like a simplistic task but depending on the nature and volume of data it can become tiresome. Most organizations would be surprised at the different types, sensitivities and volume of data they have on personal machines, servers, and databases. Purging the unnecessary data and organizing what remains in such a way that employees have access to the information they need, when they need it, without giving unnecessary access is key in this project.

It is important to ask the question “why?” while performing this analysis. Is there a better way to give employee X this information? Is accessing this information consistent with employee X’s job description? This is a very cost-effective way to begin understanding the nature of information and can inadvertently lead to the discovery of inefficiencies in processed information.

Another often under-valued step is “paranoia training.” Employees are often unaware of the information they have at their fingertips. They may not fully understand the responsibility that comes with such access. It is important for organizations to educate their employees on control measures, ways to protect the organization and the employee.

Password sharing is one of the most common failures in internal control. Logs are built on authentication and can therefore be misleading if it is a common practice in the firm to share logins. Educating employees about the risks of downloading unauthorized programs, connecting to wired and wireless networks, the importance of password changing/confidentiality, portable media and leaving laptops in cars or unattended often happens too little too late.

Other topics to consider when evaluating or developing internal controls for an organization:

- Completeness and accuracy of logs
- Application development and testing procedures
- Disaster recovery plans and contingency plans
- I.T. Personnel screening/monitoring/responsibility rotation
- Password changing procedures (e.g. Every 45-90 days)
- Antivirus and malware protection
- Email monitoring
- Encryption
- Testing environments
- Vendor access