RISK INSIGHTS Technology

EPIC

The Risks of Portable Data Drives in the Hands of Employees

Portable data drives have become a popular way to save, store and share data because they are small and very convenient. They are available at most retailers and smaller ones, like USB thumb drives, are often given away as promotional items by many companies.

However, with their increasing popularity, highly skilled technology workers may forget to err on the side of caution when using them, exposing your organization's data and systems to a security breach or malicious attack.

A Very Real Risk

The loss of confidential data due to an employee losing or misplacing a portable drive is unfortunately a relatively common occurrence. Many high profile companies have suffered a detrimental data breach like this, costing them the public's trust and expenses to repair and contain the damaging effects.

Another risk is the spread of harmful viruses through portable data drives. The Department of Homeland Security (DHS) conducted a study by placing computer discs and USB thumb drives in the parking lots of government buildings and private contractors. The test was to see how many employees would pick up and use the drives, potentially allowing unknown viruses and programs onto their equipment.

Shockingly, 60 percent of the employees who picked up the devices inserted them into their office computers. That number rose to 90 percent for devices that had a recognizable official brand logo on them. These simple actions could have exposed the organization's data and networks to a large-scale malicious attack.

Implement and Enforce

Decide on a plan of action for handling any portable data drives within your organization. Establish a protocol of password protecting and encrypting all drives to protect the sensitive data they can carry. Encryption will allow only computers with the encryption software installed to read and access the drive. This stops employees from accessing the drives on machines they are not supposed to, including home computers, preventing them from exposing the drive to harmful viruses or malware on their computer or misusing the sensitive data on the drive.

Other security measures available include biometric access technology, which requires a fingerprint scan to use the drive.

Educate and Remind

Inform your employees of the risks associated with portable data drives and your company's policy regarding how to protect them. Remind employees of these risks and policies through posters, email reminders and notes on your organization's intranet.

Create a policy regarding portable data drives and educate employees to protect against potentially hazardous risks.

Provided by David J. McNeil, ARM

877.328.4390 / 714.856.4221 david.mcneil@epicbrokers.com

RISK INSIGHTS Technology

EPIC

Data Security Through Employee Education

Data security is of the utmost importance in the technology sector. A data breach can expose your company's and your clients' highly confidential information. The results can include professional liability claims, the loss of your customers' trust and negative impact on your reputation and bottom line.

One of the first lines of defense in the fight against data loss is your staff. Implementing a strong data security training program for employees can help your company retain high standards for data protection across the organization. Well-trained and managed workers are more effective than technology tools alone.

Emphasize Continuous Caution

After undergoing education and training, employees should understand that data security is a continuous and constant concern for your organization. Instead of a one-time session, data security education should be an ongoing part of the business process. Organizations can use posters, newsletters and other reminders to keep data security issues top of mind.

Be Aware of Potential Risks

Employees are very susceptible to phishing attacks, where a hacker poses as a legitimate organization such as a client, bank or your own company. Some phishing attacks ask employees to supply confidential information such as passwords or client information to a source through an email message or website. Others try to get employees to download attachments that launch malicious software, invading all parts of their computer and eventually working its way into the company's network. Spear-phishing attacks are targeted at a small group of people, making it easier for the message to be customized and extremely convincing.

Company leaders should be aware of potential risks in order to effectively inform and train employees of their existence and how to prevent them from occurring.

Initiate and Enforce Policies

Even the best trained employee can make a mistake. Effective policies and procedures need to be in place to act as checks and balances for all data-related actions. This includes double checking and recording activities, allowing users or managers to see immediately if something was done incorrectly before any damage is done.

Following these policies and procedures needs to be part of the continuous security education to ensure their effectiveness.

Worth the Investment

The cost of not taking the time to properly train employees on data security far outweighs the investment. Professional liability claims, a third-party security audit and compliance fines are just some of the potential expenses that your company could expect if a data security incident happened in your organization.

> Training employees who handle sensitive and confidential information about data security will help decrease your company's exposure.

Provided by David J. McNeil, ARM

877.328.4390 / 714.856.4221 david.mcneil@epicbrokers.com