IT security

How companies can improve security of sensitive data

INTERVIEWED BY ROGER VOZAR

JOE COMPTON, CISSP, CISA
Principal
Skoda Minotti Risk Advisory
Services Group
(440) 449-6800
jcompton@skodaminotti.com

EVENT: Join Joe March 27 as he presents our March Speaker Series event, Technology Risk Basics: 10 Things to Improve Your Company's Technology Security. Visit Skodaminotti.com to register.

Insights Accounting & Consulting is brought to you by **Skoda Minotti**

It's difficult to protect your data when you don't know where it is and who has access.

"Most companies don't go through a data classification process. The No. 1 thing businesses can do to protect their data is to know where it is and the value it has," says Joe Compton, CISSP, CISA, a principal with the Skoda Minotti Risk Advisory Services Group.

Smart Business spoke with Compton about actions companies can take to improve information security.

How do you go about finding and classifying data?

There are many different models you can use, including a simple checklist of three things:

- Does the data contain private information?
- Should this information be restricted to a limited number of people within the organization and from outside vendors?
- Is it critical to the business? Would losing it negatively impact you or stop you from running your company?

If the data doesn't fit under any of those areas, it would be considered an unprotected asset or unimportant data.

But the model can get complex; there could be 13 or 14 categories used to organize your information. The point is to develop a data classification scheme so you can protect it. You don't want to provide the same protection for all data if it isn't necessary.

After data has been classified, what's the next step?

Once you know the data you have and its location, you need to establish controls. Most companies don't have a disciplined approach to implementing security controls.

A good source for best practices is the PCI Security Standards Council, which offers downloads that provide a detailed list of controls that should be placed around sensitive data. In the case of PCI, it deals with credit card data. Most businesses handle some sort of credit card data, but even if you don't, you could still adopt the same standards the PCI sets for credit cards and apply it to your sensitive information.

By doing so, you'll have a very disciplined and defined approach to protecting critical data sets in terms of organized controls. There's also a defined testing procedure you could follow on a regular basis to ensure those controls are working.

Controls can be as simple as firewalls or segregation of duties in terms of who has access to the data. It could involve logging access to databases and keeping a record of who works with data and where it is going. PCI has a list of 12 defined areas that it has built controls around that are appropriate for any business or any data set.

When you know what and where your data is and have a defined control set, then you need to address a data loss prevention (DLP) solution.

What are some examples of solutions, and how expensive are they?

DLP solutions range from the very expensive to relatively inexpensive.

For instance, if you run applications like SAP, Oracle financial, Microsoft Great Plains or various accounting systems, they have controls built into the software to prevent information from flowing out along with automatic tracking. But what happens when that data is moved off the system to a spreadsheet or mobile device? You can set policies prohibiting that, but that's impractical.

You want to enable people to access the data, while keeping it secure. What DLP does is make sure data is appropriately encrypted. DLP software will look inside files and, if it sees data patterns that are sensitive, will force encryption before releasing that information to a device. It will also take inventory of what was on a device. If a device that was properly encrypted is lost or compromised, you can remotely wipe it through mobile management.

There are solutions that cost a fortune, and others that cost as little as $14 per month, per user. Some are preventative — they will notify you if a mobile media device is connected to a computer and catalogue the data moved over so you know what was on the device if it gets lost.

But the first step toward a solution is identifying your data. You'll never reach the point of implementing a solution until you know what data you have and where it resides. ●