From the Business First:
http://www.bizjournals.com/columbus/print-edition/2011/01/28/rise-of-electronic-security-breaches.html

Business Law

Rise of electronic security breaches has companies on the defensive

Premium content from Business First - by Scott Rawdon , For Business First

Date: Friday, January 28, 2011, 6:00am EST

Last year was a big one for information security breaches. The biggest news didn't come out of the private sector, but rather from the publishing of sensitive U.S. government foreign relations documents by the website Wikileaks.

But the corporate side was vulnerable, too.

AT&T's website was hacked, exposing more than 100,000 customer e-mail addresses, and hackers linked to China compromised the systems of more than 30 U.S. companies, including Google, Adobe and several financial institutions.

In the information age, the ramifications of electronic security breaches for companies run the gamut – loss of revenue, legal action by customers, suppliers and partners and a damaged reputation. With more information being put out on the Internet every day, protecting it is paramount for businesses.

"Companies should have written policies regarding access to and security of data," said **Crystal Cockerell**, CEO of XLN Systems, a network security services provider based in Gahanna. "Responsible staff should be identified for developing, maintaining and implementing these policies."

getting personal

A top concern for 2011, identified by Security Week magazine, involves the privacy and confidentiality of location-based information because of the rise in use of mobile GPS information.

The magazine reports that companies will have access to information about where people and their devices spend much of their time and will have to protect employees' personal information as well as information from customers and partners. They'll also have to create policies for handling the information.

"I don't know if there are any regulatory or standards-based requirements on this," said XLN's founder, **Allen Perk**. "It's an interesting question because location-based services create the potential to track the user's movement."

XLN, founded in 1991, provides a variety of information technology services that focus on the security of corporate client networks.

Location information is especially important to businesses that collect such data for service delivery, for example. Perk thinks they should guard it well because they may be liable for any disclosure resulting in bad consequences to customers.

Location information can be inadvertently disclosed, happening as easily as posting a picture on the Internet.

"Pictures from modern electronic cameras contain GPS data that can be used to locate the home, place of work or other locations the user frequents," Perk said. If that falls into the wrong hands it could aid in a casing for a robbery.

"This can be both a business as well as a personal concern," Perk said.

Other trends, according to Security Week, include businesses choosing to encrypt more of their data, a focus on secure file transfer and creating policies for employees to explain what content is sensitive.

Luis Alcalde, an attorney with Kegler Brown Hill & Ritter LPA in Columbus with a specialty in intellectual property, said legal implications from data loss are broad. Courts so far have been reluctant to hold data possessors liable for the acts of hackers and thieves.

"I suspect the day is approaching when data possessors will be held liable for failing to maintain certain accepted industry standards to secure important electronic data," Alcalde said.

Regardless of the legal implications, he said, a company's integrity in the marketplace is almost sure to suffer following a significant security breach.

Policies to protect electronic data, including employee training programs, are becoming a must.

While most large corporations do this already, many small firms do not. "Just look at what has happened with Wikileaks, in which we're dealing with the secrets of the U.S. government," he said. "It's a constant battle in our age."

Things also are changing in the health-care industry which can make data more accessible, especially the push toward electronic health records.

But information breaches can occur in any industry, in a number of ways, said **Marie-Joelle Khouzam**, and attorney with Carlile Patchen & Murphy LLP in Columbus. A misplaced or stolen laptop, inadvertently transmitted files, employee theft or hacking by cyber criminals, for example.

Khouzam said Congress recently took steps to require a wide range of businesses to establish written identity theft prevention programs.

Scott Rawdon is a freelance writer.