



[madison.com](#) news sports opinion forums entertainment marketplace

SEARCH: all current news

ARCHIVES >>>

[\[Back\]](#) [\[Email to a Friend\]](#) [\[Printer Friendly Version\]](#)

Take Steps To Ward Off A Data Breach

Companies Must Protect Clients' Personal Information

Wisconsin State Journal :: CAPITAL REGION BUSINESS JOURNAL :: 2

Tuesday, January 1, 2008
Story by Ellen Williams-Masson

With one futuristic swipe of a finger, you can check out a new realm of data security along with a cartful of groceries at your local Cub Foods.

The Stillwater, Minn.,-based chain of 76 grocery stores switched to the "Pay by Touch" biometric payment system two years ago for added security and convenience during financial transactions. Customers who enroll in the program link their accounts with an authentication process that is unique, handy and lifelong – their fingerprint.

When a fingertip is scanned by the biometric system, a set of data points is collected, encrypted and converted into a mathematical equation. This unique verification, which can never be re-engineered into the original fingerprint, is transmitted directly to Pay By Touch secure servers.

"With Pay by Touch, you are not presenting anything other than your finger, which is associated with the account you have requested to use for your payment," Cub community relations manager Lee Ann Jorgenson said.

"Unlike credit cards or checks, no one can forge your finger – it is added security that our customers appreciate."

Identity theft costs Wisconsin businesses an estimated \$900 million a year, making data protection a financial as well as moral imperative. The Federal Trade Commission estimates that identity fraud strikes 10 million Americans a year.

Helping consumers

The Wisconsin Office of Privacy Protection was launched in April 2006 to educate businesses and consumers on the prevention of identity crime. Businesses who fail to notify individuals that their personal information has been compromised may be in violation of Wisconsin law.

According to Wisconsin's data breach notification law, most businesses, municipalities and state government agencies are required to notify individuals within 45 days if any unauthorized person has acquired their personal information. The business is also obligated to notify credit reporting agencies if more than 1,000 individuals were involved in the breach.

Susan Schilz, senior regulatory specialist at the Office of Privacy Protection, said none of the businesses with reported data breaches that have worked with her office since the law was passed in March 2006 have had a data breach policy in place.

"They had no idea what to do first, including a state agency that had a data breach," Schilz said. "It really matters that they have a plan because the sooner they act, the faster the people that were affected know, and the less exposure it gets. If somebody in the company can recognize that a data breach occurred, they might be able to stop it so that it doesn't happen

Community Pages sponsored by:

Community Pages sponsored by:

somebody in the company can recognize that a data breach occurred, they might be able to stop it so that it doesn't happen for a longer period of time."

Schilz said there are some simple steps that businesses can take to prevent data breaches in the first place, the first being "understanding whether they need to collect everything that they initially gather to authenticate the consumer."

Data that is deemed necessary to save should be stored safely, with updated network and physical protections to protect the information. Schilz said having a written privacy plan and knowing what constitutes personal information is crucial to protecting customer data no matter what size a company is.

"A privacy plan can be really important and can save a business a lot of money if their employees are trained to take care of the information that's coming in," Schilz said. "The information can be on paper, it can be verbal, it can be in a voice mail communication or it can be stored in a database. We always think about data security and almost everyone goes to what computer system they are using, but it isn't just that – it's what's left on your desk at the end of the day, what's locked up and who sees what. Have some role-based rules in your company."

Crucial to banks

Associated Bank spokesman John Vigeland said safeguarding customer trust is a fundamental tenet of the banking industry.

"Providing a safe, secure environment for people's accounts and personal information is at the core of everything we do," he said. "It's important for every business, but obviously it's crucial to banks that we protect our customers' data and safeguard their accounts and their identity. A second part of that is trying to educate customers and protect them from fraud and scams."

With more than \$21 billion in assets and 309 locations throughout the upper Midwest, Associated has the most branches of any bank in Wisconsin. Vigeland said stringent policies are in place to ensure sensitive customer information is protected.

"All paper in all of our branches and corporate offices is shredded – we don't dispose in the garbage anything other than garbage," he said. "We don't share customers' data with outside parties, and data never leaves a particular building. We have really strict rules of privacy in place that if employees are working on something at home, they are not allowed to take any data with them off site."

In a heavily regulated industry, Vigeland said employee training is key to maintaining compliance.

"The bottom line is that there is constant training going on to familiarize all the employees with all of the guidelines that we operate under as far as privacy policy and practices," he said.

Thomas Schiesl, a partner in the technology risk services department of Virchow, Krause & Company, specializes in helping companies evaluate and audit risk. He said it is essential to keep an eye on the ball during times of flux since there is an increased chance of data security breaches during major initiatives or changes in management.

Companies can often deter thieves by installing "basic safeguards to stop the wide-open intrusion," discouraging would-be hackers so they move on to easier targets. Since lapses in security can also occur in-house, maintaining a clear understanding of who has access to data and how it is handled during business operations is also critical.

"An easy-to-remedy risk in the last four or five years is people using production data to test the system," Schiesl said.

Simple precautions like maintaining a clean desk and logging off while away for brief periods can protect documents from peering eyes, but all the corporate precautions in the world can't save customers from their own mistakes.

"How many people have social security numbers as the password for their online banking account?" Schiesl asked. "There are all of the human factor elements in security."

Securing medical data

University of Wisconsin Hospitals and Clinics is in the midst of a transition from paper to electronic records and employs layers of security in a best practice strategy to protect patient data.

"At the highest level, you secure your entire network infrastructure at the perimeter with firewalls and intrusion prevention devices that monitor all the traffic that goes both in and out of the network infrastructure itself," senior data security analyst Lisa Risberg said.

"At the application level, you run audit trails so that you can monitor individuals' activity in terms of their access to data. You can run reports and monitor in real time if you need to confirm that people are only looking internally at the data that they should be looking at."

End users trained to "know what proper and inappropriate use looks like" are authenticated and authorized to access data by entering identification and passwords.

Handheld wireless devices such as those used to dispense medications add an additional challenge for network security, and wireless traffic is segmented from the rest of the network. Both wireless and wired transmissions are encrypted as an additional security precaution.

"Because health care institutions like UW Hospital are governed by the HIPAA (Health Insurance Portability and Accountability Act) security rule, there is also an emphasis on some of the HIPAA requirements in our training," Risberg said. "Security is really a best practice across industries but specific to health care, you need to educate on the HIPAA privacy rule as well."

Rich Hardyman, information security administrator at Meriter Hospital, is responsible for protecting Meriter's computer systems and patient information. He is also Meriter's HIPAA security officer.







In addition to federal HIPAA regulations, hospitals like Meriter must also comply with Wisconsin privacy laws and meet Joint Commission on Accreditation of Healthcare Organizations (JCAHO) standards to remain accredited.

"JCAHO is a private, nonprofit organization who evaluates medical facility compliance based on a focused set of requirements that are long known as essential to the delivery of good patient care," Hardyman said. "To maintain accreditation, Meriter undergoes an extensive on-site review by JCAHO professionals and patient privacy standards are part of their accreditation requirements."







Schilz said protecting customer data may not be the first priority in the boardroom, but managing the company's privacy plan and keeping an eye on privacy laws can save corporate integrity as well as the company's most important asset - its customers.

"Businesses are always thinking about how they can market, what they budget for marketing, and what they do that the customer sees to get more bang for their buck, but (data security) is something that they should be dedicating some resources to - it may be the best dollar they spend," Schilz said.

:: TOP JOBS

- [Energy Efficiency Program](#) 
 - [Biotech Scientist](#) 
 - [BE YOUR OWN BOSS The](#) 
 - [Receptionist/Billing](#)
 - [HVAC Sales](#)
 - [Director of Nursing](#) 
 - [Heart and Vascular RN](#)
 - [Sleep Lab Techs](#) 
 - [RNs and LPNs](#) 
 - [Direct Service Professional](#)
- [VIEW ALL VIDEOS](#)

:: TOP JOBS

- [Energy Efficiency Program](#) 
 - [Biotech Scientist](#) 
 - [BE YOUR OWN BOSS The](#) 
 - [Receptionist/Billing](#)
 - [HVAC Sales](#)
 - [Director of Nursing](#) 
 - [Heart and Vascular RN](#)
 - [Sleep Lab Techs](#) 
 - [RNs and LPNs](#) 
 - [Direct Service Professional](#)
- [VIEW ALL VIDEOS](#)

:: SERVICES <<<

- [Subscribe](#)
- [Renew](#)
- [Sign up for EZ pay](#)
- [Temporary stop](#)
- [Account inquiry](#)
- [Delivery concerns](#)
- [Commend carrier](#)
- [Place a classified ad](#)
- [Media kit](#)
- [Digital file requirements](#)
- [Photo reprints](#)

