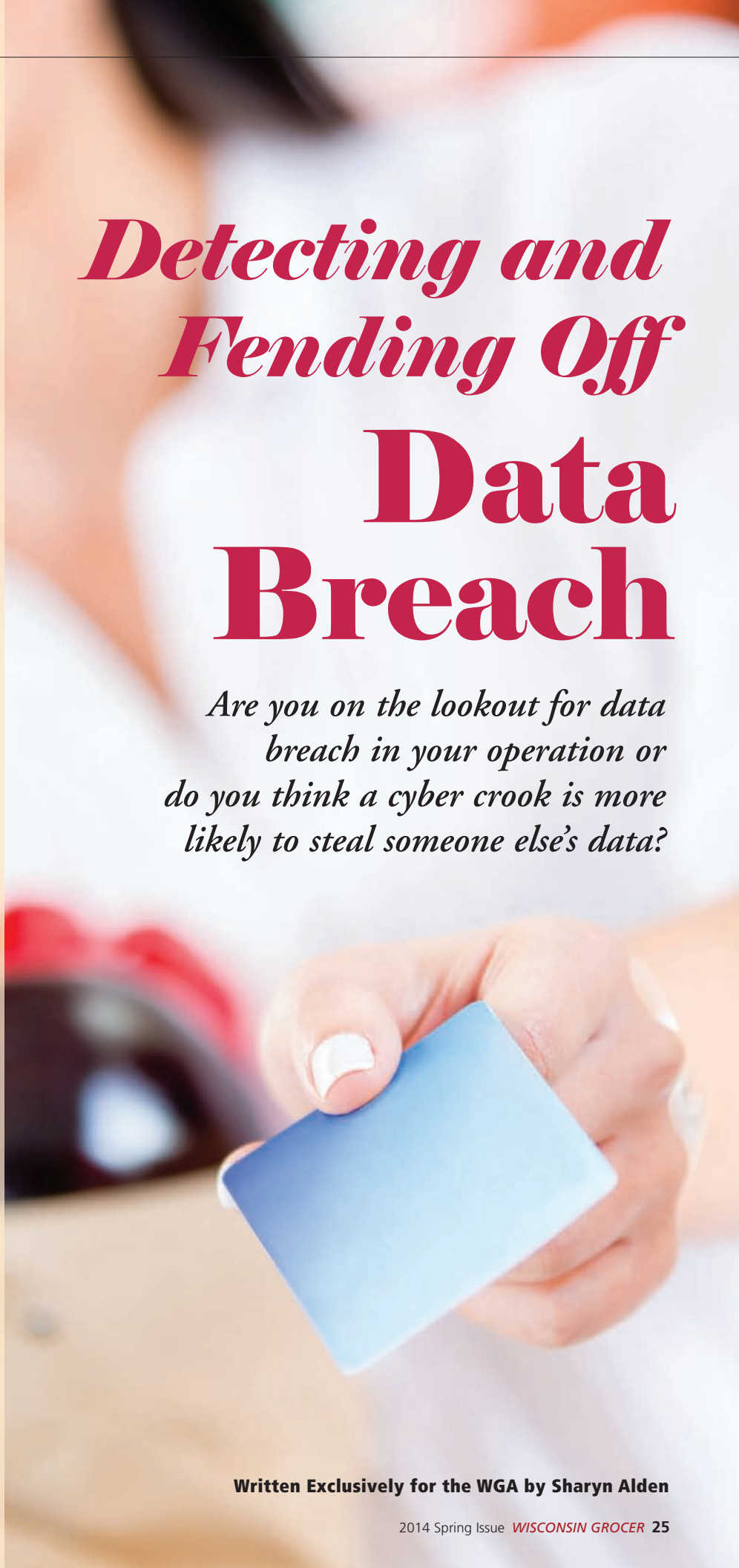
Detecting and Fending Off Data Breach

Are you on the lookout for data breach in your operation or do you think a cyber crook is more likely to steal someone else's data?



In today's business world you can't afford to be complacent about pretending data breaches can't happen to you–there's too much at stake–your sensitive data, theft of your customers' financial information as well as your store's reputation.

Warning Signs

If you are not looking for warning signs of a breach, consider this startling March 26, 2014 report. A Senate staff report from the Commerce, Science and Transportation Committee charges Target with missing multiple warning signs before hackers stole the personal information of up to 110 million customers in November and December last year.

The report called "*A 'Kill Chain' Analysis of the 2013 Target Data Breach*," says Target "failed to respond to multiple automated warnings from the company's anti-intrusion software" that not only was malware being installed on the company system, but also automated warnings that the hackers were also setting up an virtual escape vehicle, as it were, to carry away the data it was planning to steal.

This data breach along with those at Neiman Marcus, Michaels, and other retailers, have exposed how vulnerable and ill-equipped major retailers are when it comes to detecting and fending off cyber criminals.

And it raises a scary scenario: if it can happen to them, it can happen to you. If that wasn't scary enough, consider that once your data is stolen it can be copied and sold, and used over and over again, a million times over.

Don't make a mistake by turning a blind eye to the problem. Some food industry analysts say grocers should view data security at the same level of concern as food safety.

The problem is some businesses may not feel like devoting time and expenses to investing in the tightest security. Even if you're a smaller business, you too can be a

>>>

Written Exclusively for the WGA by Sharyn Alden

Bluetooth-Enabled Skimmers Reap Millions from Fuel Pumps

According to NACSonline.com article January 2014, thirteen people have been charged with stealing millions of dollars from bank data collected from illegal skimmers installed at gasoline stations in South Carolina, Texas, and Georgia. According to the court documents, by using skimming devices planted inside gas station pumps and therefore undetectable to victims who pay at the pump.

The devices are Bluetooth enabled, so the defendants did not have to physically remove the skimming devices in order to obtain the stolen personal identifying information including credit and ATM numbers, as wells as PIN numbers from these devices. Defendants are accused of fueling the fastest growing crime in the country.

Anti-Skimming Stickers

Professional Supply offers Anti-Skimming Stickers to protect you and your customers from skimming fraud. Tamper-evident stickers will help alert you and your employees to any unauthorized entries into the fuel pump cabinets. Each sticker consists of two parts and are individually numbered. Place stickers at all points of access to fuel pumps including diesel and kerosene. If someone attempts to remove the sticker or access the fuel cabinet, the sticker will show "VOID" across the front of the sticker, which will alert you to a possible fraud situation.

Professional Supply

Contact Professional Supply for additional information: (920) 565-4111.

target of cyber crooks. Smaller businesses are often attacked in an attempt to get to bigger retailers. And data breaches can spread like contagions.

There are several things businesses can do to reduce their risks to security breaches. Start by putting a strong focus on having a top-notch technology policy, understand what data you hold, who has access to it, and what part of it needs to be most secure. Encrypt your data bank securely and keep employees educated about emerging threats.

Above all else, don't become complacent. Remind yourself today that data breach is not going away.

A Wave of Breaches

Jan Gee, President of the Washington Food Industry Association (wa-food-ind.org) which represents independent grocers, says last fall 67 grocers in Washington, Oregon, Montana and Idaho were infected by a data breach. Some financial institutions noticed improper purchases but did not notify the industry due to what they perceive as liability issues. The grocers identified the problem in mid-November just as Thanksgiving shopping was heating up.

The wholesale distributor's system servicing retailers was breached at some point in the system, but the final forensic report was unable to identify as to which point the system the breached. A forensic firm hired by the wholesaler was eventually involved in the investigation with the FBI, the U.S. Treasury Department and Secret Service. "The final forensics report stated there were indicators that the 'perpetrators' were possibly from Russia," said Gee, "But the exact point where the data was stolen and by whom, is not known.

We will never protect against breaches but we can substantially reduce the opportunities for data breaches." Gee feels the credit and debit card payment processing system could be far more secure if the right tools were in place.

"We are the only 'major' developed country on earth that still uses magnetic strips on credit and debit cards with all of the customer's information embedded in the strip and not encrypted when transmitted," she said. "Because of that U.S. retailers are targets for the bad guys to steal consumer's financial information."

Mag Strip Issues

How do you make the process of swiping credit cards more secure? Financial institutions in other countries us the chip-and-pin process which is more secure than the mag strip. In fact, Gee said the U.S. Congress should mandate that the banks, retailers, and payment card processors adopt the newer chip-and-pin security standards to protect against data breaches.

"Some credit card companies have suggested converting to a chip-and-signature process but that is not as secure as the chip-and-pin system," she said.

Why hasn't the conversion happened in the U.S.? Gee pointed out that it's not the retailers – it is the financial institutions that are concerned about the cost and they claim that it is the retailers that don't want to expend the extra costs at the checkout stands. It would cost $200 - $250 for retailers to purchase the standalone equipment at each checkout stand to process the chip-and-pin cards.

The most expensive change is the cost of dedicated wiring of the processing equipment. You should not operate your computer on the same wires that you use to operate your swipe machines. This has nothing to do with the chip-and-pin, it is just a good security practice regardless if you are using the mag strip or chip-and-pin/signature.

After the Pacific Northwest grocers were breached, several additional security steps were put into place. All retailers were PCI compliant but now they must be certified by an outside company, not self-certified, and have a program in place in which an outside firm attempts to breach the system quarterly to make sure all systems are working well.

The Myth about Reimbursement Fees

"For all of us in the grocery industry, the high cost of swipe fees is something we are most concerned with," said Gee. "The credit card companies say the fees are set high to offset the cost of fraud." However, she discussed a troubling point is that fines and penalties are placed on the wholesale distributor and retailers which in part reimburse banks for the fraud losses they experienced. It's a false assumption to believe that the financial institutions are the only one paying for the fraud occurring—retailers pay also. It's also a false assumption that retailers are repaid for losses from a breach when credit card data is stolen.

Gee reiterated that this whole discussion is regarding our grocery associations – both state and national – and the need to refocus the swipe fee discussion to make it known that the card companies and financial institutions are not the only entities that experience a loss during a breach. We need to advocate policies that require the chip-and-pin and cap swipe fee fraud losses.

PCI Compliance: A Bridge to Success

The first thing to consider about PCI compliance is that it is a bridge to having a more secure operation, but it is not the end game. Jim McCool, Merchant Risk Analyst III with Shazam (shazam.net), explains, "Being PCI compliant means the merchant has attested to following all requirements developed by the PCI Data Security Standards (PCI DSS) council. That means they have completed an annual self-assessment questionnaire (SAQ) and a quarterly scan, if applicable, of their network environment through a quality security assessor."

He said it is important to remember that being PCI compliant is not a one-event situation, it is ongoing. "Keep in mind a self-assessment questionnaire is required annually, and a vulnerability scan (if applicable) is required quarterly. If there is anything that changes in how a business is processing cardholder data, PCI compliance should be reviewed."

Preventing Data Breach

Being PCI compliant doesn't guarantee your company is absolutely protected from a data breach but McCool said it does protect your cardholder data and creates awareness on the part of your business.

He added, "It can be a protection against easily avoidable threats and breaches in your network environment."

You'll also want to make sure you've achieved the two main components of validation. McCool says that means first completing the PCI-Self-Assessment Questionnaire every year. Secondly, you need to undergo a vulnerability scan performed by an approved scanning vendor every quarter.

If you think you have had a data breach, notify your merchant acquirer immediately. McCool said they will provide next steps in the process and that includes locking down operating systems. "The merchant should also be prepared to assist bank card associations, forensic investigators and law enforcement," he said.

...it is important to remember that being PCI compliant is not a one-event situation, it is ongoing. "Keep in mind a self-assessment questionnaire is required annually, and a vulnerability scan (if applicable) is required quarterly.

Keep in mind that no matter what the size of your operation, you may be vulnerable to a security breach. McCool added, "Security breaches do not just happen to mega retailers. Criminals are quickly learning that smaller businesses may be just as profitable and easier to hit than the mega merchant."

Staggering Costs

Kevin Wondra, Corporate Marketing Manager at Society Insurance (societyinsurance.com), said there are several ways to tighten your company's security starting with data breach insurance coverage.

Society Insurance offers protection for

>>>

Twelve Requirements of the PCI DSS

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

3. Protect stored cardholder data.
4. Encrypt the transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

7. Restrict access to cardholder data on a need-to-know basis.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

Maintain an Information Security Policy

12. Maintain a policy that addresses information security.

For more information visit www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

costs associated with the accidental exposure of sensitive customer data due to hacking, theft, and accidentally releasing data. "The risks and costs associated with dealing with a data breach can be extraordinarily expensive. Class action lawsuits typically seek more than $5,000 a person who was exposed."

But those costs are just starting points for how much a data breach can cost your business. Wondra said there may be costs for an internal investigation (average cost $14,000), regulatory compliance ($125,000), or notification and crisis management ($28,000).

If you have 1,000 records exposed, for example, the costs are staggering. Multiply that by hundreds or thousands of customers and you can see that costs like these can put some companies out of business.

Make sure your employees understand how to keep data secure. Then consider purchasing an insurance policy that will typically cover numerous costs associated with the aftermath of an expensive breach.

The *Wall Street Journal* recently reported that Target incurred $61 million in fourth-quarter expenses relating to their data breach, and insurance covered about $44 million of the costs. "About two-thirds of their costs were covered, and that's not bad," said Wondra who teaches a course called "The Society Coverage Difference" that highlights their data breach product to insurance agents in Wisconsin, Iowa, Illinois, and Indiana.

Make sure your employees understand how to keep data secure.

How Well are You Protected?

What exactly is a data breach? Wondra said three terms often get misinterpreted. First, **identity theft** involves thieves targeting individuals to obtain credit cards and financial information. **Cyber liability** targets businesses that accept credit cards online so they can hack into their systems and steal their financial information. **Data breach**, on the other hand, is the exposure of customer information.

"A data breach usually happens in three ways," said Wondra. "It can happen through theft such as stealing a laptop or zip-drive with sensitive information on it, hacking, or accidental release of data. If any of these occur and a business is negligent in delivering a standard of care, it needs to be proven."

Society Insurance pays for a wide variety of costs from a data breach including administration costs, such as complying with state and federal notification requirements, notification costs–preparing, printing, mailing, postage, and delivery of notification letters—and reimbursement of monitoring services that allow recipients to monitor their credit or public record files.

How Breaches Happen

How can businesses protect sensitive data? Some of the obvious solutions involve being aware of where you keep laptops. "We are moving more and more into a mobile world so backtrack and think how your data might be exposed. Could your data be exposed on laptops your employees take home?"

While many businesses have a designated IT person on staff, you may also want to bring in an outside security person. "When you're upgrading computers don't forget to install the most recent security upgrades on your smart phones as well," said Wondra. "This is another area where breaches can happen."

Wondra said if you have a breach you may also find banks respond in different and not always consistent ways.

The bottom line is what are you potentially leaving open that could constitute a data breach of customers' credit or debit cards. Consider the fall-out. "If information is breached, you have to notify every customer who also may have had their information compromised. It has to be done in a time sensitive manner and it is a very costly operation."

It's not only costly in dollars and cents, it can do irreparable harm to a company's reputation. If you do it right, your customers will likely stay with you. If you don't do it right, and even if a customer's credit card information wasn't compromised, that customer may think twice about shopping at your store again. From their perspective, it just seems like a risky place to do business.

Review Your Operation's Security

Wondra suggested the following areas to review on a regular basis.

- Educate employees; keep them aware of risk and exposure by communicating about the topic on a regular basis.
- If you have a data protection plan (you should have one) do you know where the data goes when it leaves your business? Ask your vendor or credit card processor if they have a data protection security plan to protect their data and find out what type of protection they carry.
- If you have data stored on mobile devices how strong are the passwords? Are they encrypted?
- Stay aware of every changing new possibility for data theft.

"By not protecting your company, by doing nothing, you put yourself at great financial risk and risk damaging your reputation," said Wondra. "It's hard to read a news story that describes a data breach when the company had no protection in place. The breach will likely cost the company a huge amount of money, but it doesn't have to be that way if they had built in security planning in their operation."

At the end of the day you have to ask yourself, are you doing everything you can to protect your customers' credit and debit card information? Are you doing all you can to protect your company's sensitive information from thieves?

If you have any doubts, it's time to do an extensive security review of your operation.

Sharyn Alden is a Madison-based writer who has contributed articles to the *Wisconsin Grocer* magazine for ten years, as well as to more than 200 newspapers and magazines. Sharyn covers topics such as finance, health law, travel and general consumer topics. She has written two books, *Up North Wisconsin* and *Historical Wisconsin Getaways*.