Heed Consulting Group Insight

Small Businesses : The Cost of a Data Breach Is Higher Than You Think

Introduction

In the wake of numerous recent merchant data breaches, the National Retail Federation is making a push for the adoption of EMV "chip and PIN" cards in the U.S., and merchants will need to start updating point-of-sale (POS) equipment. However, EMV alone does not ensure that payment data is fully protected, and until magnetic stripe cards are retired for good, merchants like you need to consider a multi-layered approach for protecting the sensitive cardholder data that customers entrust you with every business day.

Did you know it's possible for your business to experience a serious data breach even if you do not store cardholder data after a transaction? Cyber criminals have become quite adept at breaking into merchants' POS systems that capture and forward electronic payments. Today's attacks have become quite sophisticated, and criminals have found many points where data passing through your system is vulnerable to theft.

90%

OF BREACHES IMPACT SMALL BUSINESS

Magnetic stripe data is an attractive and frequent target of fraudsters. Stolen data easily can be printed onto other plastic cards and used elsewhere to make swiped card payments. Data thieves target small businesses in the hope and expectation that card security will be lax. Unfortunately, they are often right. According to Trustwave research, 90% of data breaches impact small merchants. A 2012 Trustwave security report indicates that Retail (45%), Food and Beverage (24%), and Hospitality (9%) are the top three compromised industries

Have you ever thought about what it would mean to your business if a payment data breach were to happen? In fact, a breach doesn't even have to be confirmed but simply suspected in order to turn your business upside down. While the financial costs can be high, even the non-monetary consequences of a data breach can be quite damaging.

Out-of-pocket expenses add up quickly

It's very rare for a small merchant to discover for itself that payment data has been stolen. Most events are detected by a law enforcement agency or a third party such as a bank or a card association that has begun to notice a rise in fraud that can be traced back to a specific merchant. When a breach of payment data is reported (or even suspected), it kicks off a series of unavoidable and costly actions that range from forensic analysis of the merchant's payment system to mandatory reporting requirements.

Small Merchants: The Cost of a Data Breach Is Higher Than You Think

If your business is unfortunate enough to have this happen, you can expect to incur significant expenses. For example, the cost of a data breach for a small business merchants averages $36,000 and can reach or exceed $50,000. Your actual out-of-pocket cost will depend on the following factors:

$36k+

AVERAGE COST OF A DATA BREACH FOR SMALL BUSINESS

- **A mandatory forensic examination** — The regulations of the Payment Card Industry Data Security Standard (PCI DSS) require that a merchant that is even suspected of having a data breach undergo a forensic examination to determine if a breach has actually occurred and, if so, to what extent. You will need to hire an outside examiner to conduct the investigation, which may last from days to weeks. This examination may require the shutdown of your point-of-sale system during that time in order to preserve evidence. According to Verizon Business, a small business examination may run in the range of $20,000 to $50,000.
- **Notification of customers** — Most states require that customers, and in many cases the state attorney general, be notified if financial information is suspected of being compromised in a data breach. Depending on the number of customers and their locations, the process of sending notifications may cost thousands of dollars. What's more, you may have to send written letters to each customer multiple times to ensure adequate communication with them.

  Though not a retail breach, the University of North Carolina at Chapel Hill said a 2013 data breach of just 6,000 records has cost the school nearly $80,000 in working with affected parties. The external costs calculated to date include $32,000 for notification letters; $22,069 for credit monitoring; and $25,000 for operating a call center.
- **Credit monitoring for affected customers** — You may be required to provide up to a year's worth of credit monitoring and/or counseling services to customers affected by your breach.
- **PCI compliance fines** — In 2011, 96% of the merchants experiencing a data breach had not complied with the PCI DSS. If the forensic investigation shows that your business was not in compliance with the industry regulation at the time of your breach, the payment card associations and/or your acquiring bank may levy fines against your business, especially if the cards have been used in actual fraud cases. Such fines for small merchants can range from $5,000 to $50,000 or more.
- **Liability for fraud charges** — Many merchants assume they have no liability for the fraudulent use of payment cards after a data breach. This is not necessarily the case; lawsuits may claim liability on merchants for security breaches.
- **Card replacement costs** — Card issuers may require that you pay the cost of reissuing debit and credit cards of those customers whose data has been compromised. These fees can range from $3 to $10 per card.
- **Upgrade or replacement of POS system** — Depending on what is uncovered to be the source of the breach, you may have to invest in upgrading or replacing your POS system, including servers, software and/or card swipe devices.
- **Reassessment for PCI compliance** — Once you have repaired or replaced your POS system, in order to qualify to accept payment cards again, you must undergo a complete PCI assessment by an external Qualified Security Assessor (QSA).

And these are just the direct costs of experiencing a data breach! There are indirect non-monetary consequences that can be just as or even more damaging to your business.

Small Merchants: The Cost of a Data Breach Is Higher Than You Think

Non-monetary damages are painful too

The out-of-pocket expenses listed above are just the start of your headache. Consider how else your business is likely to be affected.

- **Damage to your brand and business reputation** — Consumers who use their payment cards at your establishment place a high level of trust in your business, and that trust can be broken with just one breach event. In a Ponemon Institute study on breach notification, 57% of the people who had received a breach notification letter from a business said they lost trust and confidence in the organization. Worse, 31% of those surveyed said they terminated their relationship with the responsible organization. In a separate Ponemon study, three-quarters of the executives whose companies had experienced a customer data breach said the event had a significant or moderate impact on the business' reputation

31%

OF CUSTOMERS TERMINATED THEIR RELATIONSHIP

Regardless of the cause of the breach, your company shouldn't even think about claiming to be a "victim" in the breach. Consumers aren't likely to see your company as a victim if their own data has been put at risk. According to Visa, from a consumer's perspective,the issue is relatively simple: "I gave my information to you, you exposed/lost it, and it's your fault. Period.

- **Bad press** — Closely tied to brand damage is what public relations experts call "bad press." The obsessive nature of 24-hour news and social media add to the likelihood that people will hear about the misfortune of your data breach, no matter how small it is. For example, a small community liquor store in Minnesota had a relatively small breach in which a few hundred credit and debit cards were compromised. While this isn't exactly national news, information about this specific event can readily be found on the Identity Theft Resource C enter website, on a security service provider's website, on a news syndication website, and on the websites for local radio and television news stations. So if you think a small retailer's data breach won't garner much attention, think again. Unfortunately, once this information is posted to the Internet, it's there indefinitely and search engines can bring it up repeatedly.
- **Loss of payment card privileges** — Once your company suffers a data breach, credit and debit card companies such as Visa, MasterCard, American Express and others can refuse to do further business with you. Are you prepared to have a cash-only business? How many of your customers would reduce the value of their ticket or take their business elsewhere if they can't use their payment cards?
- **Your time** — As this article has pointed out, a data breach diverts a lot of attention from the daily activities of running a business to the nightmarish process of recovering from the event. If your time is normally devoted to serving your customers and overseeing normal business operations, you can expect to delegate that work to others while you (and perhaps other employees) respond to the breach.

Conclusion

Data theft processes evolve quickly, and your approach to security needs to keep up. The best way to protect your business is with a thorough and ongoing data security program. A little preventative work goes a long way, so check with your payments provider on whether they are armed with solutions that will help protect you and your customers.

Heed Consulting Group has a range of security solutions for merchants. Talk to your Heed Business Consultant to lean about affordable, easy to deploy security solutions that can mitigate potential cyber attacks and secure your customers' transactions from start to finish.

11903 0514