SAFEGUARDING YOUR BUSINESS *from a* CREDIT CARD BREACH

NTC Texas
Payment Processing

NTC Texas
Payment Processing

SAFEGUARDING YOUR BUSINESS *from a* CREDIT CARD BREACH

TABLE OF CONTENTS

Published by NTC Texas, May 1, 2015

INTRODUCTION

Cyber theft has become the bank robbing of the 21st century. Gone are the days of revolvers, "put the money in the bag" heists, and the chance to stop the criminals before they make a get-away. With the exchange of money becoming a primarily virtual industry, criminals have adapted. The good news: fewer traumatized bystanders. The bad news: getting away with it is easier than ever.

While businesses are well aware of the threat, especially considering the number of high profile breaches that have occurred within the last three years, the challenge of protecting credit card and personally identifiable information (PII) is daunting. Hackers, who accounted for almost 30 percent of data breach incidents in 2014, seem to thrive on circumventing well-planned security measures and have managed to make off with billions of records within the last several years—and not all from big businesses who can afford to compensate consumers for their losses.

"LARGER BUSINESSES ARE NOT THE ONLY TARGETS FOR CYBER THEFT, A FACT THAT MANY SMALL BUSINESSES FAIL TO CONSIDER."

Larger businesses are not the only targets for cyber theft, a fact that many small businesses fail to consider. In fact, according to the National Small Business Administration, **virtual theft cost small businesses an average of $8,699 per attack as of late 2013, and nearly half of those surveyed in the 2013 report had experienced at least one attack.** Considering that the Identity Theft Resource Center reported a 27.5 percent increase in cyber-attacks in 2014—and that 33 percent of all breaches were in the business sector—it's not a large logical leap that small businesses are in more danger from cyber criminals than ever before.

Combatting the threat of cyber theft is vital for businesses of every size. While some of the more advanced technology to battle these threats can be costly or complicated, there are many ways to secure your data and prevent breaches—not all of which require high up-front costs. Often, just having the right information makes a difference. If technology expenditures are necessary, consider them an investment; the added security will promise both peace of mind and greater protection to your consumers and your bottom line. In the following brief, you will see examples of past breaches, to both large and small businesses, as well as additional security practices that will help keep your business safe in the years to come.

CASE STUDIES
Examples of Big Business Breaches

Home Depot Affecting a total of **56 million cards over 5 months,** the incident became the second largest breach in history, surpassing Target's breach in 2013 by 16 million cards. Even more, the company announced in November of last year that **53 million email addresses had been compromised at the same time, exposing customers to possible phishing attacks** in the future, although no password or other sensitive information was affected.

In response, Home Depot has implemented a new system that enhances encryption of card data, making them "virtually unreadable," according to a report released by the company, and has offered free identity protection services to any customer who paid by card in 2014. Officials are also speeding up the rollout of EMV machines, a process the company had started for U.S. stores in early 2013.

Target Beginning Black Friday weekend of 2013, the retail super chain suffered a breach that continued for 10 days before officials were notified of malware in their system. Reportedly, they only found out due to a leak from the website of a black market cyber thief named Rescator. The breach itself occurred through malware that found its way into Target's refrigeration system, which was apparently connected to the same internal systems that housed Target's POS machines.

According to Bloomberg Business, **Target's security system detected the malware before the attack, but somehow tech security officials failed to notice the warning displays**–a mistake that has cost Target millions of dollars and immeasurable amounts of consumer confidence. In total, 40 million credit card numbers and **70 million email addresses were stolen.** Disconcertingly, the stolen email addresses and other compromised personally identifiable information (PII) affected more than just 2013 shoppers. Paula Rosenblum, a contributor to Forbes, wrote that she had received "the letter" even though she hadn't shopped in-store or online for over a year.

Target officials have since assured consumers that they are taking security measures to prevent any repeat incidents. The primary step will be implementing EMV technology in both their store POS systems and within the REDcards they issue directly to customers.

Examples of Smaller Business Breaches

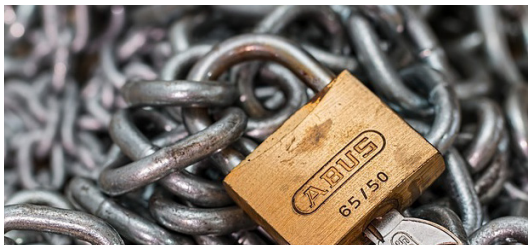
Kirkwood Community College On March 13, 2013, **hackers using an international IP address accessed archived application information from February 2005 to March 2013.** The compromised details included everything from **applicant names, birthdates, and race to social security numbers.** No financial data or academic details were affected.

The small college in Cedar Rapids, Iowa responded by immediately shutting down the website, contacting local and federal law enforcement, and engaging a specialized firm to help investigate and fortify the school's systems. Officials also **offered free identity protection and restoration services to all who were affected.**

OnlyHonest.com A small internet-based business started by Michael Hopkins, OnlyHonest.com allowed users to debate political topics via video uploads. Just before the company's year anniversary, individuals affiliated with a hacker group known as **Anonymous defaced every page of the website.** When Hopkins attempted to remove the "graffiti" and regain control over the site, the attacks moved to redirecting all internet traffic to a different site.

Hopkins attempted to raise money through a crowd funding project on rockethub.com to rebuild and protect from future hacking attempts, but the website is no longer operational today, most likely as a direct result of the hacking since all media associated with the site has been untouched since 2013.

General Security Practices for All Businesses



Effectively safeguarding your business requires a combination of preparation and vigilance. Understanding the threat, complying with the industry's standardized security practices, and committing to communication and strict focus on maintaining secure internal practices are all essential aspects of preventing cyber theft in your business.

"EFFECTIVELY SAFEGUARDING YOUR BUSINESS REQUIRES A COMBINATION OF PREPARATION AND VIGILANCE."

Understand PCI Regulation. As the owner of a business that accepts credit cards, you should be aware of Payment Card Industry (PCI) regulations. The PCI Security Standards Council was founded by American Express, Discover Financial Services, JCB, MasterCard and Visa Inc. in 2006 to create best practices for the industry. Adhering to PCI regulations will help you protect your consumers and help secure the future of your business.

Per the PCI security standards, businesses must maintain several levels of technological security, including firewalls, regularly updated anti-virus software, and network resource access tracking, as well as encryption—among several others.

Most importantly, **PCI calls for regular vulnerability and self-assessment tests to ensure the systems are working as they should**—so breaches like those described above don't happen to you. For help complying with these standards, see our PCI compliance page.

Document Security Procedures

It's all fine and well that PCI offers a ready-made roadmap for protecting your business, but you have to make it your own. For the changes to truly stick, you need to **create your own internal security guidelines that adhere to these standards but are tailored to the specific needs of your business.** Write the details into your training manuals, into your policies and procedures documents, and into any quick reference guides your employees might use.

Most importantly, these regulations, procedures, and standards should be discussed with employees, and they should be trained to make good choices. According to the 2014 Ponemon Cost of Data Breach Study, **30 percent of data breaches were related to simple human error.** Don't be part of next year's statistic.

Do Not Store Certain Card Data

PCI regulations forbid any storing of both "track data" and the three- to four-digit security codes on the backs of cards. If you are storing data electronically, do not create storage fields for these numbers. If these numbers are written on paper, be sure to destroy them after use.

Properly Store Other Information

At times, mail-order payments or recurring payment authorizations may require additional card holder information. **Do not give into the information-hoarding temptation.** Try to only keep the bare minimum of information. Opt for a payment processing solution that allows you to store data for recurring payments in a secure environment, there are many affordable software based processing solutions that have this function. Electronic files should also be encrypted, or tokenization should be used.

Tokenization

Tokenization takes data and replaces it with unique identification symbols for transfer through electronic networks. For merchants, this equates to maintaining no data on hand, leaving the tokenization process to a payment provider. Servers remember the unique data and recognize returning customers. Tokenization may be an easy way for your business to stay PCI compliant and eliminate any concerns about storing sensitive data.

SECURITY PRACTICES FOR IN-STORE TRANSACTIONS

In-store transactions may seem safer than ecommerce or mobile transactions, but many major credit card breaches have occurred through in-store interactions as well. Choosing equipment wisely, with an eye on proper security, is key to preventing theft.

Use PCI Compliant Equipment.

Unfortunately, not all POS machines and software are safe for use. In fact, many have vulnerabilities that can be exploited by malware or hacking. Approved hardware providers go through tough testing procedures before putting their products on the market. The PCI Security Standards Council has a list of approved vendors, which you can use to find quality products.

Use EMV Technology

"EMV" stands for **Europay**, Mastercard, and Visa and refers to a special **smart chip embedded within credit cards that protects the cardholder's personal information and account access details by ensuring that unique, random data codes are used for each transaction.** This "chip and pin" or "chip card" technology has already been tested for more than two decades in Europe and has proven reliable for decreasing instances of compromised PII and stolen card data. Businesses need a special type of credit card machine to process these cards. As part of a movement in the US to implement EMV, **businesses that are not using this technology by October 2015 will be held liable for breaches of their in-store systems.**

E-COMMERCE SECURITY PRACTICES

Although convenient for customers, "e-commerce," or online payment sites, require a whole new level of security—actually multiple levels. If your business elects to accept card payments online you'll want to step up your game on hacking and malware prevention efforts.

Use SSL Encryption

IMake sure to use strong cryptography, such as SSL (Secure Sockets Layer), across open Internet networks. SSL provides a better guarantee for secure communication between the customer and your e-commerce website.

Require Strong Passwords

If recurring customers create usernames, require that they have passwords that can withstand attack. A CISD study found that **hackers can often crack alphanumeric passwords in just minutes; adding a simple punctuation mark changes that timeframe to years.**

Set-up Firewalls

A firewall is a necessary first defense for your server. According to PCI standards, merchants should also have an additional Web Application Firewall, a more analytical firewall designed to prevent attacks specifically against web applications, for their e-commerce sites. Remember to follow through with proper set-up once installed. The United States Computer Emergency Readiness Team (US-CERT) reports that many hacked businesses made the simple mistake of not providing outbound data rules. Some even forget to change default passwords, an all too easy way to lose a lot of money really fast.

Malware and Patches

Even if you have a firewall, regularly update anti-virus software in case computers being used to manage websites are infected. Be sure to stay on top of software patches as breached sites are typically running old versions of software or code.

Continue to Check Systems

Continue checking to make sure there aren't any holes that would leave your business perimeter unprotected. Test the system on your own, or hire someone to test it for you—all in keeping with PCI guidelines, of course—just to see if you can find any weaknesses to shore up. Be on the lookout for other easily corrected ways of breaking into a system, such as leaving open remote connections, so the simple mistakes don't come back to bite you.

SECURITY PRACTICES FOR MOBILE PAYMENTS

With the rise in smartphone popularity and prevalence, mobile purchasing power is the new chic. Businesses across the world are hastening to develop apps and mobile friendly websites that make it easy for consumers to log right in and get that impulse purchase immediately, before the urgency slips away, of course. The temptation to partake in such a feast of profits is overpowering—for both business owners and cyber criminals. Even more, simple equipment add-ons to mobile phones have created on-the-go POS machines, making anytime-anywhere purchasing easier than ever—and also boosting the threat to those purchases. Maintaining security with mobile purchasing requires as many internal protections as with e-commerce and even more vigilance since mobile phones are so easily "misplaced."

"WITH THE RISE IN SMARTPHONE POPULARITY AND PREVALENCE, MOBILE PURCHASING POWER IS THE NEW CHIC."

Mobile Firewalls and Malware

Many users tend to think that phones aren't the targets of viruses. As the number of smartphone users have increased, along with the number of business transactions made through mobile devices, cell phone malware infections have also been rising. **If you are using a mobile device to process customer purchases—in-store or on the go—prepare a phone with the same caution as you would a PC. There are several mobile anti-viral and anti-malware programs to choose from.**

Clear Lost Devices

Even if you believe your business's portable devices are somehow "misplacement-proof", a smart business owner is always ready for the unexpected. Setting up security procedures (specific steps to take in the case of theft or misplacement of phones, tablets, laptops, or other portable hardware) will help immensely to increase response time and help you prevent any catastrophic attacks on your business. Having the ability to disable any payment application from a distance is always wise, especially if the device has been used as a POS.

CONCLUSION

A breach or cyber attack of any kind can damage a business financially, while simultaneously ruining both reputation and customer confidence. Target is now equated with being a "target" for hackers, for example. Small businesses still run the risk of being decimated by a few clicks and taps if they don't start taking greater precautions.

How can you keep this from happening? Building a better defense starts with understanding what you're up against, what industry experts recommend you should do about it, and what options are available that would fit best with your type of business. **Utilizing secure server locations, tested and proven payment software, several different layers of encryption, and a few specialized firewalls are all essential parts of an effective security plan.**

With the myriad of advances in technology, businesses face even greater risks. Don't let it happen to your business, especially when there are hundreds of options available for protecting businesses of all sizes against cyber attacks. Using the checklist above, a little vigilance, and a lot of determination, you can avoid being one of the thousands whose business are either virtually ransacked or practically destroyed by cyber theft. **Take the right steps today to protect your investments, and all your hard-won profits will stay right where they belong—in your secure, vaulted, firewall-protected, encrypted, password-protected virtual pocket.**

READ MORE ABOUT DATA SECURITY FROM THE NTC TEXAS BLOG

Don't Expose Yourself or Your Customers

http://www.ntctexas.com/credit-card-processing-blog/bid/61736/Don-t-Expose-Yourself-or-Your-Customers

Could Your Business Withstand a P.F. Chang's or Target Style Breach?

http://www.ntctexas.com/credit-card-processing-blog/bid/71913/Could-Your-Business-Withstand-a-P-F-Chang-s-or-Target-Style-Breach

Cybercrime, Not Terrorism, Largest Threat to U.S

http://www.ntctexas.com/credit-card-processing-blog/bid/64849/Cybercrime-Not-Terror-ism-Largest-Threat-to-U-S

NTC Texas
Payment Processing

106 Decker Court, Suite 260, Las Colinas, TX 75062
Phone (972) 406-8111 | www.ntctexas.com