Security:

Overcoming customer concerns in an increasingly uncertain digital world.

Background:
If you think the term digital security doesn’t belong in your small business dialogue — think again. 2014 was dubbed “The year of the data breach” by 60 Minutes, and hackers show no sign of letting up for 2015.

Today, we’re all members of an anywhere, anytime market place, and the customer’s increasing reliance on wireless accessibility means that all business owners — big and small — need to understand how digital security can impact business. As a small business it’s important to understand your small businesses exposure.

Let’s start by dispelling a couple of popular myths:

1 Hackers only target big business. Not according to an August 2014 New York Times article exposing a Russian crime ring with the largest known collection of stolen Internet credentials: “Hackers target any website...from Fortune 500 companies to very small websites...and most of these sites are still vulnerable.”

2 There’s little a small business can do. If big-name businesses like Target and Home Depot are struggling to maintain customer trust, there’s very little a small business can do. True, the loss of sensitive information, like credit card numbers and personal data, can be devastating to customer confidence. But there’s still a lot you can do to prevent damage to your business’s reputation.

The rules governing how and where you keep customer data depends a lot on the type of business you operate and the kind of customer information you work with. You should start by reviewing the U.S. Laws Governing Data Security to ensure you’re meeting all the legal requirements.

You should also be prepared to answer customer questions/concerns regarding your data security policies. Always be up front about your privacy policy and be clear with customers about what kinds of information you

784 new data breaches recorded in 2014
Identity Theft Resource Center

33% of attacks aimed at business
People are more comfortable shopping online. But these (cyber) attacks have everyone’s attention. Better Business Bureau Accreditation tells customers we’re part of a trustworthy organization.

Dmitriy Peregudov, Chief Gift Officer, GiftBasketsOverseas.com, BBB Accredited Business since 1/26/2009.

keep as a matter of record. And, if you don’t have a comprehensive security strategy, it’s time to develop one.

One simple and effective way to show customers you’re committed to their safety and security is to become part of a community of trustworthy businesses.

Start with Trust: Today, it’s more important than ever.

Customers know that the very tenets of the BBB Code of Business Practices (BBB Accreditation Standards)³ require businesses to secure sensitive data, such as credit card and bank account numbers, Social Security numbers, salary or other personal financial information.

The fact is, when your business earns BBB Accreditation, you’re joining one of the most well-known and well-respected organizations in the country. BBB is one of the most visited websites in the USA and Leary is part of a growing number of twenty-first century companies that are finding increasing value in becoming part of BBB.

Butcher, Baker, Cupcake Maker — customer trust is important for analog businesses, too.

The very nature of today’s business transactions makes even the most traditional retail model vulnerable to some kind of attack. The simple act of accepting credit cards could make you a target.

Mobile businesses (contractor, landscaper, cleaning service, etc.) should watch out for Wi-Fi. It’s a dangerous misconception to believe an off-line industry

“Joining the Better Business Bureau serving Eastern Massachusetts, Maine, Rhode Island and Vermont was one of the smartest business moves I’ve made.”

Judy Leary, President of IdentityForce, BBB Accredited Business since 11/30/2007.
makes you immune to criminal activity. If you take your office with you on the road — with a smart phone or tablet — you should be aware that most kinds of communication from a wireless connection can be hacked. Many Wi-Fi networks you encounter out in the real world aren’t secured. Be extra cautious in high-volume areas, such as airports, bus stations, libraries, hotels, and coffee shops. In particular, “Avoid making purchases over a wireless connection in a public space.”

“Shared connections allow hackers to lure you to fake sites where they can gather your credit information.” said Leary, of IdentityForce.

As larger companies with deeper cyber-security pockets become harder to attack, it naturally follows that smaller and smaller businesses will become targets of least resistance. In the February 2015 issue of Entrepreneur Magazine, security software business Trend Micro revealed that cyber criminals assault the small business space with 3.5 new threats every second.

“Customers just trust BBB to protect their interests...I’ve never run into a customer who didn’t know the seal and trust it!” says Nelson Miller from All Construction & Remodeling, a BBB Accredited Business.
In today’s climate of fraud and increasing digital uncertainty, it’s no wonder customers are turning to a trusted symbol of business credibility for over 100 years: Better Business Bureau Accreditation Seal.

“...there are simply too many opportunities for a misstep: a hard drive or laptop is lost or stolen, a PDA or thumb drive is misplaced, human error occurs, or a network gets hacked. A data breach can have devastating consequences: legal penalties and fees can cost millions; retailers can lose their ability to accept credit cards; and your business’s reputation and customer loyalty can be severely damaged.” say Leary.

The tools of BBB Accreditation also allow small businesses — like IdentityForce — to drive a robust customer acquisition programs. “We use the positive BBB feedback as the foundation for a successful customer acquisition strategy. That’s because personal referrals are the strongest sales tool going.” says Leary.

According to findings from a 2014 BrightLocal survey:

“Nearly 9 in 10 consumers have read online reviews to determine the quality of a local business, and 39% do so on a regular basis. The ‘trend line’ over the last four
years clearly shows how much more regularly people are reading reviews, clearly highlighting the need for local businesses to attract more reviews and actively manage their online reputation.”

Of course, you don’t have to be in the security business to benefit from BBB Accreditation. Dmitriy Peregudov, Chief Gift Officer, GiftBasketsOverseas.com, credits becoming a BBB Accredited Business as a powerful branding tool.

As a small business, you can convince customers that you are committed to a higher level of trust with BBB Accreditation. When you partner with BBB, it says you are committed to an enhanced level of credibility. Customers know and recognize BBB as a seal of excellence. It says you take customer satisfaction very seriously in every aspect of your interactions — not just when they work with you online. So, join the over 390,000 local Accredited businesses and apply for BBB Accreditation today.

“We do business in 200 countries world-wide, but over half of our orders originate inside the US. As an Internet business, we know it’s important for customers to have complete trust in our operations — the Better Business Bureau Accreditation Seal on our website does that!” — Dmitriy Peregudov, Chief Gift Officer, GiftBasketsOverseas.com, BBB Accredited Business since 1/26/2009.

Appendix:

What’s out there and how it can impact your small business.

In the New York Times article discussed earlier in this paper, Alex Holden, founder and Chief Information Security Officer of Hold Security (the Milwaukee firm that exposed a Russian crime ring), recommends “checking if your website is susceptible to an SQL injection.” SQL is the programming language that most databases use. An SQL injection happens when a hacker exploits vulnerabilities in a web site to run commands directly on the database that stores the application’s data.

45% increase in the number of smart phones infected with malware
Just by entering specially-formatted data into a field on a vulnerable form, a criminal could steal all of your data, including passwords, credit card numbers and all of your customers’ private information.

Before the discovery of the Russian crime ring, the security business Imperva stated that the average web application receives four SQL Injection attacks per month, with retailers getting twice as many as other industries. SQL injections attack websites, but they can be used to attack any type of SQL database.

SQL aside, the sad reality is you don’t need a business website to become the victim of some kind of attack. It’s the proliferation and sophistication of attacks that has analysts concerned. Cisco Chief Security and Trust Officer John Stewart discussed cyber security threats on Bloomberg West\(^5\), indicating spam was up 250%.

We’ve gone from spam to Spear Phishers (a particularly nasty category of email that angles to steal your financial information) and the next battleground is right in your customer’s pocket.

Malicious smart phone apps, sometimes known as *Ransomware*, can literally take a smart phone hostage. Sound like science fiction? Not according to Lookout CTO and Co-Founder Kevin Mahaffey. In a January 2015 interview with Bloomberg BusinessWeek\(^6\), Mahaffey said, “The largest risk to the individual is downloading a bad app...they’ll take your data, take your money...it’s one of the biggest trends in the US. The number of smart phones infected with some kind of malware in the US went from 4% to 7% annualized.”

### Recent Hacks

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>60 million</td>
<td>payment accounts compromised at Home Depot</td>
</tr>
<tr>
<td>76 million</td>
<td>households (plus 7 million small businesses) left vulnerable by JPMorgan Chase</td>
</tr>
<tr>
<td>110 million</td>
<td>shoppers compromised in Target hack</td>
</tr>
<tr>
<td>200 million</td>
<td>Social Security, credit card and bank account numbers snatched by Vietnamese theft service</td>
</tr>
<tr>
<td>1.2 billion</td>
<td>username &amp; password combinations plus more than 500 million email addresses stolen by Russian crime ring</td>
</tr>
</tbody>
</table>

**Who can customers count on?**

Better Business Bureau recently launched a “Look For the Seal” campaign asking shoppers to check for the Better Business Bureau Accreditation Seal and properly research a business before making a decision to buy.

Who can customers count on?

Who can customers count on?
What’s next: Malware in our microwaves?

As funny as that sounds, more and more of our everyday devices (current examples include automobile sensors, smart thermostats, washer/dryers, etc.) utilize Wi-Fi for remote monitoring. Often called The Internet of Things (IoT), these interconnected devices rely on the existing Internet’s infrastructure to relay information. Gartner, Inc., a technology research and advisory corporation, believes there will be nearly 26 billion devices on the Internet of Things by 2020, and that could present an attractive target for the criminal element.

That said, you can rest assured that hackers won’t be invading your break room microwave anytime soon. This has less to do with feasibility and more to do with monetization. Just like the businesses they target, the majority of hackers are in it to make money. And there’s no money in hacking appliances — yet.

2015: The year of the ram...or the rampaging hacker?

The new Chief Technologist at the FTC, Ashkan Soltani, has set his sights on enhancing the agency’s efforts, saying, “Data Security is one of the most important aspects of a functioning marketplace and a critical aspect in consumer protection.”

Despite record spending on cyber/data security ($4 billion+), the Identity Theft Resource Center reports 784 new breaches for 2014 — with 33% of that aimed at the business sector. Small wonder that Adobe’s Chief Security Officer Brad Arkin blogged “…cyber attacks are one of the unfortunate realities of doing business today…” after his business was targeted.

The numbers are breathtaking: 110 million shoppers were compromised in the Target hack, 60 million payment accounts were compromised at Home Depot, and 76 million households (plus 7 million small businesses) were left vulnerable at JPMorgan Chase. In October 2014, federal prosecutors identified a theft service in Vietnam that managed to obtain up to 200 million personal records, including Social Security numbers, credit card data, and bank account information. New York Times reports of a Russian crime ring with the largest known cache of stolen Internet
credentials: 1.2 billion username and password combinations and more than 500 million email addresses.

Obviously, it’s time to ensure your small business is protected. Once you have reviewed the U.S. Laws Governing Data Security, take a look at the additional links below. Many may be useful for assessing your vulnerabilities. You can also research BBB Accredited Business Directory for companies that specialize in cyber security.

Additional free small business resources:

U.S. Small Business Administration: Cybersecurity training for small businesses
https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses

Federal Trade Commission: Protecting personal information. A guide for business:

Federal Communications Commission: Ten cybersecurity tips for small businesses

Small Biz Cyber Planner:
http://www.fcc.gov/cyberplanner

Consumer Reports: Internet Security Guide

FBI: How to Protect Your Computer
http://www.fbi.gov/scams-safety/computer_protect

OnGuardOnline, a US Government site dedicated to helping small businesses protect data, networks, and IT systems:

PrivacyRights.org: Chronology of Data Breaches
http://www.privacyrights.org/data-breach/new

IdentityForce: How to outsmart hackers

IdentityForce: How to protect credit card data from hackers

“Spam is up 250%”
John Stewart, Cisco Chief Security and Trust Officer on Bloomberg West
Links to videos/articles discussed in this paper:

1 August 2014, New York Times article:
http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?_r=0

2 U.S. Laws Governing Data Security:

3 BBB Code of Business Practices (BBB Accreditation Standards):

4 2014 BrightLocal survey:

5 Cisco Chief Security and Trust Officer John Stewart discussed cyber security threats on Bloomberg West:
http://www.businessweek.com/videos/2015-01-20/will-companies-change-cybersecurity-strategies

6 Kevin Mahaffey CTO and Co-Founder January 2015 interview with Bloomberg BusinessWeek:
http://www.businessweek.com/videos/2015-01-20/bad-apps-can-take-money-hold-phone-hostage-mahaffey#r=search_result